RÉSEAUX TÉLÉCOM

WIFI PROFESSIONNEL

La norme 802.11, le déploiement, la sécurité

SUPPLÉMENTS en ligne

Aurélien Géron

Préface de Marc Taieb

3e édition

DUNOD

WIFI
PROFESSIONNEL

La norme 802.11, le déploiement, la sécurité

Aurélien Géron

Cofondateur et directeur technique de Wifirst

Préface de Marc Taieb

3e édition

DUNOD

Illustration de couverture :
Lake Jackson © Ronnie Howard - Fotolia.com

ISBN 978-2-10-054183-6

Préface

Sévèrement touchée par l'aventure UMTS, l'Europe a cherché des solutions économiques à la transmission de données sans fil. Elle a su trouver une voie honorable en proposant des services sur la norme Wireless-Fidelity. Les usages ont été déclinés à la maison, au bureau, dans la rue et dans les « zones blanches ».

Les constructeurs y ont décelé un relais de croissance et les opérateurs, généralement frileux, ont fini par leur emboîter le pas. En 2002 la technologie était confidentielle, aujourd'hui la France compte des milliers de points d'accès. La presse, friande de sujets leur rappelant la grande époque de la « bulle », ne tarit pas d'éloge pour cette forme de cabine téléphonique d'accès haut débit. Certains ont même imaginé une France couverte en WiFi.

Les technologies sans fil existent depuis des dizaines d'années, avec des débits croissants et des bandes de fréquences de plus en plus rares. Les normes ont donc évolué pour optimiser et simplifier les plages. Si le GSM a été capable de transporter de la voix pour 75 % des habitants (moyenne européenne), les transmissions de données génèrent moins de 10 % des revenus et doivent s'adosser à d'autres normes comme la 3G et le WiFi. À l'heure où la 4G pointe son nez, nous savons que le WiFi ne sera pas une parenthèse de l'histoire de la haute technologie.

En dépit des rumeurs des plus acides qui ironisaient sur le débit et la sécurité des réseaux sans fil le standard 802.11 a surpris par sa stabilité et sa simplicité. Le livre d'Aurélien GÉRON cristallise, dans une démarche pédagogique, la différence entre le WiFi et la perception que l'on peut en avoir. Peu d'ouvrages ont su décrire avec autant de précision l'état réel de cette technologie. Il était nécessaire d'inscrire la norme dans une photo plus grande qui la positionnait face aux autres normes sans fil et qui légitimait sa prédominance. Cette tâche a été acquittée sans quitter du regard les problématiques de sécurité.

Je tiens enfin à saluer la rigueur de l'ouvrage et de son auteur, que je connais personnellement et à qui je voue une grande admiration, tant pour ses qualités de travail que pour sa créativité.

Marc TAIEB
Cofondateur et directeur de la société Wifirst

Table des matières

Deuxième partie – Déploiement

Avant-propos

La technologie WiFi fait parler d'elle

La promesse d'un monde sans fil est alléchante : se connecter à Internet sans le moindre câble, à la maison, au bureau, voire même dans des points d'accès publics appelés *hotspots*. Les rêveurs y voient le nouveau « boom » des Technologies de l'Information et de la Communication (les TIC), à la mesure du succès qu'a connue la téléphonie mobile grâce à la technologie GSM. Les sceptiques, rendus méfiants par le « flop » des « .com » et la crise des télécoms, n'y voient qu'une mode qui doit passer aussi vite qu'elle est arrivée, remplacée rapidement par une autre technologie plus prometteuse, moins coûteuse ou simplement mieux commercialisée.

Légitimes dans un premier temps, on peut maintenant affirmer que ces craintes ne sont plus justifiées. En effet, au-delà des rumeurs exaltées (le « buzz »), le WiFi a réellement conquis le grand public. Les grands opérateurs proposent dorénavant des abonnements ADSL avec des modems WiFi pour se connecter n'importe où à la maison. Les fabricants d'ordinateurs portables ont franchi le pas et la grande majorité de leurs produits est dorénavant compatible WiFi. Des géants se sont lancés à corps perdu dans la bataille, à l'image d'Intel qui a investi massivement dans la mobilité avec sa technologie Centrino, compatible WiFi.

Le WiFi pour l'entreprise

Les entreprises, timides au début par crainte des nouveaux problèmes de sécurité que posent les réseaux sans fil, ou attendant simplement la maturité de la technologie et des produits, sont maintenant en train de prendre la vague du sans fil. Les intérêts pour l'entreprise sont en effet importants : les coûts de câblage peuvent être très largement réduits ; les employés, équipés d'ordinateurs portables compatibles WiFi, peuvent rester connectés et productifs hors du bureau ; les réunions sont plus faciles à organiser car le réseau est disponible partout et pour tout le monde ; les réaménagements de bureaux sont nettement moins complexes à gérer ; les clients, fournisseurs et autres visiteurs peuvent se connecter facilement. Toutefois, concevoir et maintenir un réseau WiFi d'entreprise, sécurisé, rapide, disponible dans tous les bureaux et bien administré, est une autre gageure que de connecter quelques ordinateurs à un réseau WiFi familial et peut très vite virer au cauchemar.

Objectif de ce livre

Comme son nom l'indique, ce livre a pour but de présenter le WiFi de façon aussi exhaustive que possible, pour les entreprises désireuses de passer au WiFi, mais aussi pour le particulier passionné par les technologies ou le simple curieux. Autant les ouvrages dédiés au grand public abondent, autant un responsable informatique ou un administrateur réseau est aujourd'hui démuni lorsqu'on lui demande de « wifiser » son entreprise et qu'il cherche la littérature adaptée (en français, en tout cas). D'excellents ouvrages détaillent les rouages du protocole lui-même. D'autres décrivent les solutions de sécurité en vigueur actuellement. Quelques-uns traitent de l'optimisation de la couverture radio. Mais très peu offrent une synthèse pratique et complète. C'est cette lacune que cet ouvrage a pour but de combler.

Contenu des chapitres

Ce livre est composé de trois parties chacune centrée sur un thème :

- *Comprendre le WiFi* : chapitres 1 à 3
- *Déployer votre réseau sans fil* : chapitres 4 et 5
- *Sécuriser votre réseau sans fil* : chapitres 6 à 11

Première partie : comprendre le WiFi

La première partie a pour but de vous apporter une bonne compréhension du WiFi : vous saurez ce qu'est le WiFi et comprendrez les rouages de la norme 802.11.

Le chapitre 1 présente une vue d'ensemble du WiFi, son contexte historique, technique et commercial et ses principales applications.

Les chapitres 2 et 3 détaillent la norme 802.11 sur laquelle repose le WiFi. Le chapitre 2 se concentre sur les couches physiques et présente les variantes du WiFi : 802.11a, 802.11b, 802.11g et 802.11n. Le chapitre 3 présente la couche MAC du protocole 802.11, c'est-à-dire le " cerveau " du WiFi, qui offre de nombreuses fonctionnalités essentielles, telles que la sécurité ou encore le partage des ondes.

Deuxième partie : déploiement

La seconde partie doit vous permettre de bien préparer et réaliser le déploiement de votre réseau sans fil.

Le chapitre 4 présente le matériel WiFi, des adaptateurs WiFi aux points d'accès (les AP, c'est-à-dire les bornes WiFi) en passant par les antennes et les téléphones WiFi. Des conseils pratiques sont proposés pour mieux choisir votre matériel.

Le chapitre 5 traite de la couverture radio. Il permet de savoir comment déployer les AP et positionner les antennes pour obtenir un réseau performant en fonction du contexte : connexion de point à point, réseau d'entreprise simple, réseau à haute capacité, etc.

Troisième partie : sécurité

La troisième partie présente les solutions permettant de sécuriser votre réseau WiFi.

Le chapitre 6 offre une vue d'ensemble de la problématique de sécurité dans un réseau sans fil et présente quelques-unes des solutions simples pour un niveau élémentaire de sécurité.

Le chapitre 7 présente la solution WEP. Il s'agit de la première solution de sécurité proposée par le standard 802.11, malheureusement complètement insuffisante. Toutefois, elle est encore très répandue et doit donc être présentée.

Le chapitre 8 détaille le protocole 802.1x dont le rôle est d'identifier les utilisateurs et de préparer une connexion sécurisée. Ce protocole simple et générique est à la base de nombreuses solutions de sécurité dont le WPA Enterprise.

Le chapitre 9 présente en profondeur le WPA, la solution " miracle " du WiFi, qui offre un niveau de sécurité sans fil exceptionnel. Les deux architectures possibles sont détaillées : le WPA Personal pour les particuliers ou les très petits réseaux, et le WPA Enterprise pour les réseaux plus conséquents.

Le chapitre 10 présente le protocole RADIUS et explique comment mettre en place et configurer un serveur RADIUS. Ce serveur est l'un des composants des solutions de sécurité basées sur le 802.1x, dont le WPA Enterprise.

Le chapitre 11 aborde enfin les obligations légales que vous devrez respecter si vous déployez un réseau WiFi, notamment la protection de la vie privée des utilisateurs, la lutte anti-terrorisme et la sécurité sanitaire (ce dernier point étant détaillé).

Les annexes

Ce livre comporte quatre annexes qui présentent des sujets divers, utiles pour comprendre certaines parties de cet ouvrage, mais trop éloignés du WiFi proprement dit pour figurer au sein d'un chapitre, elles sont disponibles sur le Web (www.livrewifi.com ou www.dunod.com) :

- **L'annexe A décrit les réseaux IP**, l'adressage, le routage et les principaux protocoles. Cette annexe est importante pour toute personne qui ne serait pas déjà familière avec ces notions. Si vous ne savez pas ce qu'est une adresse IP, un paquet TCP ou une requête ARP, cette annexe est faite pour vous.
- **L'annexe B présente l'attaque ARP**, qui est le point de départ de plusieurs attaques permettant à un pirate de compromettre la sécurité de votre réseau. Elle illustre à quel point les pirates sont créatifs et combien ils peuvent nuire.
- **L'annexe C présente les certificats électroniques**, le cryptage asymétrique et les protocoles TLS et SSL.

À la fin de ce livre, vous trouverez un glossaire et un index. La quantité astronomique de sigles et de termes techniques qui fourmillent dans les domaines de l'informatique et des réseaux est telle que le glossaire, qui contient plus de 200 définitions, sera sans doute utile assez fréquemment. Chaque sigle est néanmoins décrit dans le texte, lors de sa première utilisation.

Comment lire ce livre ?

Ce livre peut être lu comme un roman (bien qu'il ne prétende pas au prix Goncourt), c'est-à-dire de la première à la dernière page. Toutefois, la plupart des chapitres sont conçus pour pouvoir être lus relativement indépendamment. Il est recommandé de lire en premier le chapitre 1 : il offre une vision globale du WiFi. Les chapitres 2 et 3 présentent la norme 802.11 en détail, vous pouvez donc les survoler pour vous faire une idée générale de cette norme et y revenir si vous avez besoin de comprendre un point particulier. D'autre part, il est préférable de lire les chapitres 8, 9 et 10 dans l'ordre, en prenant un bon café avant de vous lancer.

Tous les chapitres se terminent par un résumé d'une ou deux pages, qui rappelle les points essentiels à retenir. Si un chapitre vous ennuie, lisez simplement son résumé ! Par ailleurs, de petits encarts soulignent les points les plus importants au cours de chaque chapitre.

Cet ouvrage sera je l'espère à la fois un guide pratique pour l'entreprise ou le particulier souhaitant s'équiper d'un réseau WiFi robuste et sécurisé, et un manuel sur l'état de l'art de la technologie.

Vous trouverez l'ensemble des annexes, les références et les commentaires sur *www.livrewifi.com*.

Remerciements

Je tiens à remercier vivement Emmanuelle Tessier, pour sa grande patience, son soutien, ses relectures attentives et ses conseils avisés. Merci également à ma famille et à mes amis, que j'espère voir davantage maintenant que ce livre est terminé !

Je remercie l'équipe Wifirst, pour son extraordinaire énergie, sa bonne humeur et son efficacité. En particulier, un grand merci à Marc Taieb, Leif Stevenin, Arnaud Puy et Arno Pical pour leur précieux soutien pendant l'écriture de cet ouvrage. L'œil de lynx de Leif m'a évité bien des coquilles !

Je tiens également à remercier l'équipe des éditions Dunod, Jean-Luc Blanc, Carole Trochu et Sébastien Bago, pour leur dynamisme, leur gentillesse et la qualité de leurs relectures et commentaires.

Un grand merci à Michel Tessier qui m'a aidé à ne pas aggraver les choses dans le match (hum...) entre le français et l'anglais.

Merci également à Emmanuel Curis qui a eu la gentillesse et la patience de relire et corriger l'ensemble de cet ouvrage avec une minutie rare : des virgules en trop aux questions de propagation des ondes radio, rien ne lui a échappé. Je lui en suis profondément reconnaissant.

Les modulations radio n'ont aucun secret pour Adrien Demarez : j'ai eu la chance de pouvoir bénéficier de ses cours particuliers improvisés qui n'avaient rien à envier aux meilleurs cours magistraux. Il était parfois relayé par Michel Chevallier, qui m'a apporté une aide précieuse pour le dernier chapitre en compilant une riche bibliographie sur les effets des ondes sur la santé. A tous les deux je tiens à dire merci !

Un clin d'œil à Tristan Boureau, pour ses sessions de travail acharné, son optimisme et son esprit « Mouduge ».

Pour finir, je remercie affectueusement mon frère Sylvain Géron qui m'a propulsé dans l'aventure du WiFi.

PREMIÈRE PARTIE

Comprendre le WiFi

Ces trois premiers chapitres ont pour but de vous apporter une bonne compréhension du WiFi :

- le chapitre 1 présente le WiFi, son contexte historique, technique et commercial, ses applications et les technologies alternatives ;
- le chapitre 2 présente les couches physiques définies par la norme 802.11 sur laquelle repose le WiFi. Les différentes variantes du WiFi (802.11a, 802.11b, 802.11g et 802.11n) sont abordées en détail ;
- le chapitre 3 présente la couche MAC définie par la norme 802.11 : il s'agit du « cerveau » du WiFi, qui lui apporte de nombreuses fonctionnalités.

1

Contexte et applications du WiFi

Objectif

Ce premier chapitre a pour but de présenter brièvement l'histoire de la technologie WiFi, son contexte technique, ses applications principales et les technologies concurrentes : le lecteur novice aura ainsi une vision d'ensemble de la technologie et de sa finalité.

1.1 UN BOOM À RETARDEMENT

1.1.1 De l'histoire ancienne

La naissance des ondes

Le « sans fil » est à la mode aujourd'hui. Pourtant, c'est déjà de l'histoire ancienne. Cette histoire commence à la fin du XIX^{e} siècle avec la découverte des ondes électromagnétiques par le physicien allemand Heinrich Hertz en 1888. Dix ans plus tard, le 5 novembre 1898, Eugène Ducretet, assisté d'Ernest Roger, établit la première communication radio à « longue distance », sur 4 kilomètres, entre la Tour Eiffel et le Panthéon : c'est le début de la Télégraphie sans fil (TSF). En 1908, ces ondes radio transportent déjà la voix et la musique, grâce à Lee de Forest ! Deux ans plus tard, celui-ci retransmet même un opéra donné au Metropolitan Opera House à New York : c'est l'une des premières émissions de radio. En 1924, John Loggie Baird retransmet sur les ondes des images d'objets en mouvement, à la Royal Institution. Encore deux ans plus tard, il permet à un visage humain de s'afficher pour la première

fois sur un écran de télévision *via* les ondes radio : la télévision hertzienne est née. Les techniques se perfectionnent tout au long du siècle et en particulier pendant la deuxième guerre mondiale : certaines des techniques du WiFi sont d'ailleurs nées des recherches militaires.

Les réseaux sans fil

Puis vient l'ère du numérique. Le premier véritable réseau numérique sans fil date de 1970 : cette année-là, des chercheurs de l'université de Hawaï sous la direction de Norman Abramson réunissent les technologies radio et les technologies numériques de communication par paquets de données. Il s'agit du réseau sans fil AlohaNet. Pour la première fois, plusieurs ordinateurs sont reliés entre eux grâce aux ondes radio. Ce réseau sans fil s'offre même le luxe d'une connexion par satellite à Arpanet, l'ancêtre de l'Internet créé en 1969 !

1.1.2 Les raisons du retard

Alors si ces technologies sans fil ne sont pas nées de la dernière pluie, pourquoi la vague du sans fil ne déferle-t-elle sur nous qu'aujourd'hui ? Les réponses sont multiples.

Faible débit

D'une part, les débits des connexions sans fil ont toujours été loin derrière ceux des connexions filaires (fig. 1.1). Il a longtemps fallu se contenter de quelques kilobits par seconde (kb/s) ce qui n'était pas comparable aux débits des réseaux filaires où l'on parle depuis longtemps en mégabits par seconde (Mb/s). Encore aujourd'hui, le WiFi permet au mieux d'atteindre quelques centaines de mégabits par seconde, alors que le filaire peut atteindre sans difficulté le gigabit par seconde (Gb/s), voire même le térabit par seconde (Tb/s)[1].

Solutions propriétaires

En outre, les produits disponibles n'étaient généralement pas standardisés (on parle de solutions « propriétaires ») ce qui interdisait le plus souvent l'interopérabilité entre les offres des différents fournisseurs. Cela signifie qu'en choisissant une technologie donnée, on était dépendant d'un constructeur unique, qui pouvait disparaître ou encore imposer des tarifs excessifs.

Réglementation

Par ailleurs, la réglementation sur les ondes radio a également ralenti le développement du sans fil pour les réseaux d'entreprise. Les ondes radio étant par nature une ressource limitée, chaque pays définit des règles que les émetteurs doivent respecter.

1. Le débit d'un lien numérique se mesure en nombre de bits d'information (0 ou 1) par seconde que l'on peut échanger : 1 kb/s = 1 024 b/s, 1 Mb/s = 1 024 kb/s, 1 Gb/s = 1 024 Mb/s, 1 Tb/s = 1 024 Gb/s.

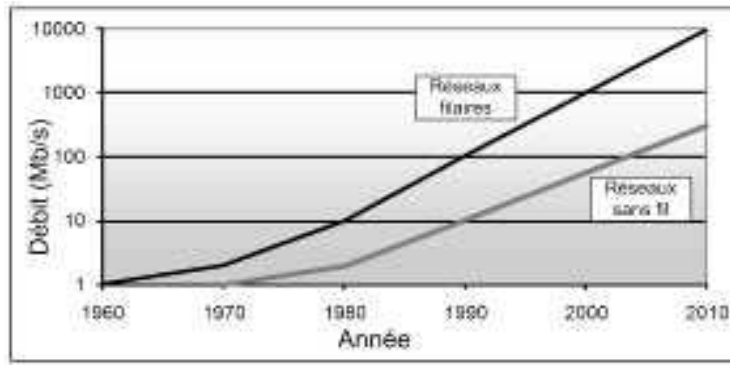


Figure 1.1 — Débits des réseaux filaires et sans fil.

Malgré des efforts d'homogénéisation, ces règles varient beaucoup d'un pays à l'autre. Elles fixent en général une puissance rayonnée maximale, imposent parfois d'acheter une licence pour avoir le droit d'émettre, voire même précisent quelle technologie radio utiliser.

L'intérêt de ces réglementations est d'éviter que les émissions des uns ne brouillent celles des autres, de permettre un partage « équitable » des ondes radio et de limiter l'impact des ondes sur la santé. Des bandes de fréquences sont donc définies et réservées à certains usages : télévision, radio, communications militaires, etc.

En France, c'est l'Autorité de Régulation des Communications Électroniques et des Postes (ARCEP), anciennement appelée l'Autorité de Régulation des Télécommunications (ART), qui a la responsabilité de définir ces règles et l'Agence Nationale des Fréquences (ANF) a pour rôle de les faire respecter, en effectuant des contrôles réguliers et en distribuant des amendes dissuasives aux contrevenants.

Seules quelques bandes de fréquences assez limitées sont libres pour tout usage et sans licence, en respectant tout de même une limite de puissance[1]. En France, ce n'est que fin 2002 que l'ARCEP a décidé de libérer complètement la bande de fréquences radio de 2,4 gigahertz (GHz) sur laquelle reposent les normes WiFi 802.11b et 802.11g (fig. 1.2). Encore aujourd'hui, il faut se contenter d'une puissance d'émission de 10 à 100 milliwatts (mW) ce qui limite fortement la portée des équipements[2]. Le WiFi 802.11a, qui fonctionne sur la bande de fréquences radio de 5 GHz, était tout simplement interdit à l'extérieur et limité à l'intérieur à 200 mW seulement jusqu'en janvier 2006. Il est maintenant autorisé à l'extérieur sous certaines conditions, comme nous le verrons plus loin. Le 802.11n peut être utilisé sur les deux plages de fréquence à 2,4 GHz ou à 5 GHz, mais de nombreux adaptateurs 802.11n ne gèrent que l'une des deux fréquences, le plus souvent le 2,4 GHz.

1. Voir les tableaux synthétiques concernant la législation au chapitre 11.
2. À titre de comparaison, notons qu'un simple téléphone portable a en général une puissance supérieure à 1 Watt, soit 1 000 mW, donc dix fois plus qu'un point d'accès WiFi.

Le prix

Dernier frein du sans fil et non des moindres : le coût des équipements était très élevé, ce qui rendait prohibitif l'installation d'un réseau sans fil dans la majorité des contextes, en particulier pour les réseaux d'entreprises. L'absence de standard explique en grande partie ce coût élevé : si chaque constructeur utilise sa propre technologie, il doit utiliser des composants spécialisés produits uniquement pour lui, c'est-à-dire en relativement faibles quantités, donc chers. Inversement, si tous les constructeurs appliquent le même standard, les composants utilisés seront « communs » et bon marché.

> **Résumons** : faible débit, coût élevé, absence de standard, législation hétérogène et contraignante... Bref, on comprend mieux pourquoi le sans fil a tant tardé à connaître le succès.

1.1.3 Le boom du WiFi

Mais mieux vaut tard que jamais : à la fin des années 1990, la situation avait beaucoup évolué. L'essor de la téléphonie mobile avait commencé à sensibiliser le grand public aux technologies sans fil. Les réglementations en matière d'ondes électromagnétiques commençaient à s'assouplir et, dans une certaine mesure, à s'homogénéiser dans le monde.

Un standard

Mais surtout, en 1997, l'*Institute of Electrical and Electronics Engineers* (IEEE) ratifiait son premier standard 802.11 qui promettait des débits théoriques[1] de 1 à 2 Mb/s sur différents médias : soit la lumière infrarouge[2], soit les ondes radio de fréquence 2,4 GHz. Cette bande de fréquences radio a l'avantage d'être utilisable sans licence dans de très nombreux pays et c'est surtout pour cette raison qu'elle a été choisie. À peine deux ans plus tard, en juillet 1999, l'IEEE publia le 802.11b qui apportait une amélioration importante du débit sur les ondes radio à 2,4 GHz : on pouvait dès lors atteindre des débits théoriques de 11 Mb/s, ce qui devenait tout à fait comparable aux connexions filaires. Dès la fin 1999, les premiers produits respectant cette norme arrivaient sur le marché, à des prix relativement bas et qui allaient très vite encore baisser.

1. Le débit théorique est le nombre maximum de bits transmis par seconde au niveau physique (radio). Le débit réel, toujours plus faible, est le débit observé par l'utilisateur. Avec la technologie WiFi, le débit réel est environ égal à la moitié du débit théorique. Ceci est dû aux erreurs de transmission, à la redondance de certaines informations, aux silences entre l'envoi des paquets de données, etc.

2. Il n'existe pas à ce jour de produits au standard 802.11 reposant sur la lumière infrarouge, aussi nous ne détaillerons pas cet aspect du WiFi. En outre, l'*Infrared Data Association* (IrDA) a défini des standards infrarouges plus performants et pour lesquels il existe de nombreux produits.

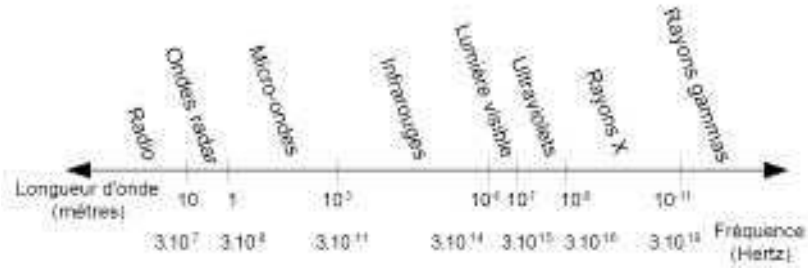


Figure 1.2 — Le spectre électromagnétique : le WiFi repose sur les micro-ondes.

Une association de constructeurs

Comme si tout cela n'était pas assez, la *Wireless Ethernet Compatibility Alliance* (WECA) vit le jour la même année. Il s'agit d'une association à but non lucratif composée de plus de 200 acteurs du marché du sans fil et dont le but est de promouvoir les produits respectant les normes sans fil de la série 802.11. Connue aujourd'hui sous le nom de *WiFi Alliance*, cette association a eu un rôle majeur dans le succès actuel du WiFi (*Wireless Fidelity*[1]). L'une de ses premières actions a été de définir un ensemble de contrôles de qualité et des tests d'interopérabilité permettant de garantir qu'un produit respecte bien les normes de l'IEEE et qu'il peut s'interconnecter avec des produits d'autres fournisseurs. Un produit passant ces tests avec succès reçoit le label WiFi qui est un gage de qualité et d'interopérabilité (fig. 1.3). À ce jour, plus de 5 000 produits ont reçu ce label, ce qui démontre à la fois le succès du WiFi et celui de la WiFi Alliance. Notons qu'à l'origine, le terme WiFi désignait uniquement le label de qualité, mais par extension, il est à présent employé pour désigner la technologie elle-même.

> L'IEEE a créé le standard 802.11 pour les réseaux sans fil.
> La WiFi Alliance a créé le label WiFi pour les produits 802.11.

Grâce en grande partie à la WiFi Alliance, le WiFi est donc très rapidement passé du papier à la réalité et les produits ont vite gagné en stabilité et maturité. L'une des nombreuses raisons du succès du WiFi est en effet la qualité des produits : en bref, grâce aux contrôles qu'ils doivent subir pour obtenir leur label de qualité, ils fonctionnent, dans l'ensemble, très bien.

Enfin, une fois tous ces critères réunis, prix, maturité, standard, débit, législation et grâce aussi à une bonne couverture médiatique, la « masse critique » a été dépassée, ce qui a entraîné et entraîne encore aujourd'hui et de plus en plus vite, l'effet « boule-de-neige ». Voyons donc maintenant plus précisément en quoi consiste le WiFi.

1. C'est-à-dire « fidélité sans fil ». Il s'agit d'un jeu de mot en référence à la qualité *High-Fidelity* ou Hi-Fi du monde audio.

Figure 1.3 — Le logo de certification de la WiFi Alliance.

1.2 QUELQUES RAPPELS SUR LES RÉSEAUX

Comme dans tous les domaines des Technologies de l'Information et de la Communication (TIC), le WiFi croule sous un jargon opaque de sigles, de surnoms, d'abréviations et de numéros de versions. Ceci peut dérouter n'importe qui. Afin de vous éviter ces déboires, cette section se propose donc de clarifier brièvement les termes et les concepts fondamentaux des réseaux que nous allons utiliser tout au long de ce livre. Nous revenons ici sur des notions de base des réseaux telles que le modèle OSI et les couches de protocoles. Si vous savez déjà ce qu'est un protocole de niveau 2 ou 3 et ce que sont les PAN, LAN, MAN, WAN et les WLAN, alors vous pouvez allégrement passer au § 1.2.5.

1.2.1 Les réseaux et les protocoles

Selon la définition du *Petit Robert*, un réseau est « un ensemble de points communiquant entre eux ». Dans le monde numérique, ces « points » ou « nœuds » du réseau sont des équipements informatiques. Il peut s'agir d'ordinateurs bien sûr, mais aussi d'imprimantes, de systèmes de vidéosurveillance, de téléphones portables ou de tout autre matériel électronique. On parlera de « périphérique », d'« hôte » ou de « station » pour désigner ces équipements. La « topologie » du réseau représente l'agencement des nœuds entre eux : des réseaux peuvent être organisés en boucle, en arborescence, en mailles, etc.

Afin que ces stations puissent communiquer entre elles, il est nécessaire d'une part qu'elles sachent exploiter un média de communication adapté (des câbles électriques ou optiques, des ondes radio, la lumière infrarouge...), mais aussi et surtout qu'elles soient capables de se synchroniser et de se comprendre. Pour cela, des règles de communication doivent être définies. Le rôle d'un standard réseau est donc de définir des protocoles (c'est-à-dire les modalités précises) de communication entre les périphériques d'un réseau : quand prendre la parole, comment définir qui s'adresse à qui, etc.

1.2.2 Les couches de protocoles

Une façon de concevoir les protocoles réseaux tels qu'ils existent aujourd'hui est de les comparer à une société très hiérarchisée où chacun ne communique qu'avec des personnes d'un rang directement supérieur ou inférieur. Par exemple, si le directeur

souhaite envoyer un message au directeur d'une autre société, il le dictera à sa secrétaire de direction, qui le tapera et le transmettra au stagiaire pour relecture, celui-ci vérifiera les éventuelles fautes d'orthographe et transmettra la lettre à l'accueil, ce dernier mettra la lettre sous pli et la donnera au livreur qui effectuera enfin la livraison. Bien sûr, à destination, on peut imaginer un processus identique pour réceptionner l'enveloppe, la décacheter, vérifier son contenu et la fournir au directeur (fig. 1.4). Comme on le constate, à chaque niveau correspond une tâche très précise, ce qui permet de limiter la complexité (donc le coût) de chaque composant individuel, d'augmenter la fiabilité de l'ensemble et de garantir une certaine indépendance entre les composants.

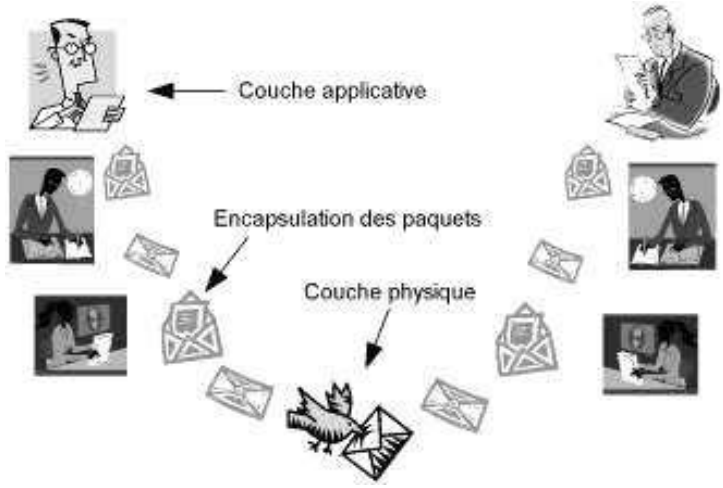


Figure 1.4 — Vision schématique des couches de protocoles.

C'est ce type d'architecture par couches superposées (appelées *layers* en anglais) qui domine dans le monde des réseaux d'aujourd'hui. L'utilisateur est au sommet de la pyramide (il correspond au directeur dans notre exemple précédent). Il communique avec la couche réseau la plus « haute », en général au travers d'un logiciel (ou « application ») tel qu'un navigateur Internet par exemple. Ces applications mettent en œuvre la « couche applicative ». Celle-ci communique elle-même avec une couche moins élevée et ainsi de suite jusqu'à la couche la plus « basse », à savoir la couche physique, qui peut utiliser un câble de cuivre, une fibre optique, de la lumière infrarouge ou encore des ondes radio.

Évidemment, l'analogie s'arrête là : le processus de livraison complet dans une telle société pourrait prendre plusieurs heures, vu le nombre de personnes par lesquelles le message doit passer, alors que dans les réseaux informatiques, chaque intermédiaire est si rapide que les messages s'échangent en général en quelques millisecondes.

Lorsque l'on parle des performances d'un réseau, il faut distinguer le débit et le temps de latence : le débit est la quantité d'information pouvant être transmise par seconde et le temps de latence est le temps nécessaire pour que cette information arrive à destination. Sur une autoroute, il peut passer plusieurs milliers de voitures par

heure (c'est le débit), mais une voiture donnée mettra plusieurs heures pour parcourir son trajet (c'est le temps de latence).

1.2.3 Le modèle OSI

Un standard de l'*International Organisation for Standardization* (ISO) a été publié en 1979 pour définir comment les couches réseaux doivent être organisées et ce qu'elles doivent faire : il s'agit du standard *Open Systems Interconnection* (OSI). Il propose sept couches :

- **Niveau 7 : la couche applicative** – Il s'agit du service réseau offert à l'utilisateur, tel que l'envoi ou la réception de courrier électronique ou la navigation web. Cette couche est mise en œuvre par des logiciels.
- **Niveau 6 : la couche de présentation** – Elle se charge de coder les données envoyées par la couche applicative en un format indépendant de la machine.
- **Niveau 5 : la couche de session** – Elle se charge de négocier les conditions d'une session de communication entre deux hôtes, de créer cette session et de la détruire une fois que la communication est terminée (sur demande de la couche de présentation).
- **Niveau 4 : la couche de transport** – Elle se charge de découper en petits paquets les données trop volumineuses et de rassembler ces paquets à l'arrivée (en les remettant au besoin dans le bon ordre). Un contrôle des éventuelles erreurs de transmission peut avoir lieu ici.
- **Niveau 3 : la couche réseau** – Elle s'occupe d'acheminer les paquets entre différents réseaux. On parle de « routage » des paquets.
- **Niveau 2 : la couche de liaison de données** – Elle s'occupe de détails techniques tels que le contrôle d'erreur et le partage du support de communication.
- **Niveau 1 : la couche physique (notée PHY)** – Elle s'occupe de la transmission des données proprement dite. Elle précise en particulier le type du média de communication, le format des éventuels connecteurs à utiliser, la définition exacte des paramètres physiques qui doivent être interprétés comme des « 1 » et des « 0 » : par exemple le voltage d'une impulsion électrique ou la fréquence d'un signal radio.

Ce modèle semble assez générique et élégant et il a donné l'espoir de voir un monde des réseaux simple et unifié. On pensait que tous les constructeurs allaient vite adhérer à ce modèle, mais cela n'a pas été le cas. En partie pour des raisons d'optimisation des communications et en partie par manque de précision dans la définition des couches OSI (vous l'aurez sans doute remarqué !), les couches des protocoles réseaux actuels ne correspondent qu'approximativement au modèle OSI. Certaines couches sont coupées en deux, d'autres sont regroupées, d'autres se chevauchent. En outre, certaines fonctions comme la sécurité ou le contrôle d'erreur sont mises en œuvre par plusieurs couches à la fois. Le modèle OSI est donc aujourd'hui essentiellement employé à des fins pédagogiques : il aide à comprendre comment les réseaux sont organisés et à classifier les protocoles, mais il n'est pas rigoureusement mis en pratique.

En ce qui nous concerne, le plus important est de savoir que le WiFi ne concerne que les couches 1 et 2 du modèle OSI. Il définit donc précisément quel média utiliser (couche 1) et comment des paquets de données doivent être échangés au sein d'un même réseau (couche 2), mais il ne s'occupe pas du routage des paquets entre différents réseaux, par exemple. De même que le livreur ne se préoccupe pas du contenu des paquets qu'il livre, le protocole WiFi peut transporter n'importe quelles données correspondant à des protocoles de niveau supérieur ou égal à 3 dans le modèle OSI. C'est le cas en particulier du protocole Internet (*Internet Protocol*, IP) qui est de niveau 3.

> La norme 802.11 définit uniquement les couches 1 et 2 du modèle OSI : la couche physique et la couche de liaison de données.

1.2.4 La typologie des réseaux

Les réseaux sont classifiés en fonction de leur étendue. Cela va de l'interconnexion entre quelques équipements situés à quelques centimètres les uns des autres à un réseau d'échelle planétaire comme l'Internet.

Un exemple de protocole réseaux très répandu est l'Ethernet. On le trouve maintenant dans presque tous les réseaux d'entreprise. Il se situe au même niveau que le WiFi (couches 1 et 2 du modèle OSI) et est également standardisé par l'IEEE (sous le numéro 802.3). Il permet à des stations de communiquer entre elles par le biais de câbles en cuivre (les câbles réseau les plus communs) ou en fibre optique à des débits pouvant aller jusqu'à 10 Gb/s ! La longueur de ces câbles peut aller de quelques mètres à plusieurs dizaines de kilomètres (grâce à la fibre optique), mais le plus souvent, tous les éléments d'un même réseau Ethernet se situent dans un espace de moins de 200 mètres de diamètre, suite à des contraintes techniques liées au protocole Ethernet lui-même (voir le chapitre 3, § 3.1.4). Plus généralement, les réseaux Ethernet ne sont pas conçus pour gérer des milliers d'utilisateurs sur des distances importantes et c'est pourquoi l'on parle de « réseaux locaux » ou *Local Area Networks* (LAN).

Plusieurs réseaux locaux peuvent toutefois être reliés entre eux grâce à diverses technologies pour former un réseau de plus grande taille. À l'échelle d'une métropole, on parle de *Metropolitan Area Network* (MAN). On les trouve par exemple dans des campus universitaires où ils regroupent les LAN des différents bâtiments, ou encore entre les stations de métros d'une ville comme Paris. Dans ce cas, d'autres protocoles que l'Ethernet, tels que l'*Asynchronous Transfer Mode* (ATM), sont souvent employés pour relier les LAN entre eux[1].

En allant encore plus loin, on atteint des réseaux qualifiés de « larges » ou *Wide Area Networks* (WAN). Le plus connu est bien sûr l'Internet qui relie entre eux une grande partie des réseaux du monde entier. Autre exemple, lorsqu'une société internationale relie ses bureaux entre eux, en passant ou non par Internet, on parle également de WAN.

1. Le Gigabit-Ethernet sur fibre optique est également souvent utilisé à l'échelle d'un MAN.

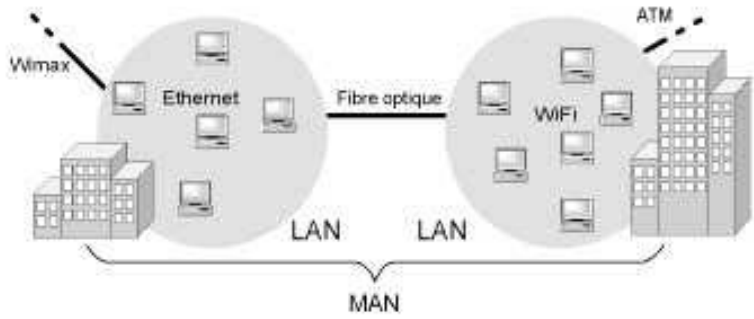


Figure 1.5 — Réseaux locaux (LAN) et réseau métropolitains (MAN).

À cette échelle, les chemins possibles pour aller d'un point à un autre sont souvent multiples. Lorsqu'un paquet de données est émis en un point, il est donc nécessaire d'appliquer des règles de routage pour l'acheminer à bon port. C'est le rôle d'un protocole de niveau 3 dans la couche OSI et le plus souvent, on choisit IP.

À l'opposé des WAN, l'interconnexion entre quelques équipements très proches les uns des autres, comme par exemple un clavier sans fil et un ordinateur, constitue un *Personal Area Network* (PAN). L'espace occupé par un PAN, souvent centré sur l'utilisateur, est parfois appelé le *Personal Operating Space* (POS).

> Les réseaux sont classés par leur taille : PAN < LAN < MAN < WAN

1.2.5 Les WLAN

Pour sa part, le WiFi a été conçu, comme Ethernet dont il s'est inspiré, pour mettre en œuvre des réseaux locaux, mais, bien entendu, en s'affranchissant des fils grâce à la magie des ondes électromagnétiques. On parle donc de *Wireless LAN* (WLAN), c'est-à-dire « LAN sans fil », à ne pas confondre avec WAN bien sûr. On parle aussi de *Radio LAN* (RLAN) si le support de communication est la radio (et non la lumière infrarouge par exemple).

Les stations du réseau sans fil peuvent communiquer directement entre elles, on parle alors de réseau de type Ad Hoc, ou par le biais de bornes relais appelées des points d'accès (*Access Points*, AP) : il s'agit alors d'un réseau de type *Infrastructure*. Le second type est de loin le plus fréquent en entreprise.

> Il existe deux types de réseaux WiFi :
> – les réseaux de type Ad Hoc, où les stations communiquent directement entre elles ;
> – les réseaux de type Infrastructure, où les stations communiquent par le biais de points d'accès.

Pour communiquer, chaque station doit bien sûr être équipée d'un adaptateur WiFi et d'une antenne radio (souvent intégrée dans l'adaptateur). De plus en plus

d'équipements informatiques sont vendus avec un adaptateur WiFi intégré. Si ce n'est pas le cas, il faut en acheter un et le connecter à la station. La connectique est très variée : il existe des adaptateurs WiFi USB, PCMCIA, PCI, etc.

Il existe plusieurs variantes du WiFi, sur lesquelles nous reviendrons en détail au cours du chapitre 2. En deux mots, le 802.11b et le 802.11g sont compatibles entre eux et fonctionnent tous deux avec les ondes radio d'une fréquence de 2,4 GHz. Le 802.11b atteint un débit de 11 Mb/s et le 802.11g monte à 54 Mb/s. Le 802.11a n'est pas compatible avec le 802.11b et le 802.11g, car il fonctionne avec les ondes radio d'une fréquence de 5 GHz. Il permet d'atteindre 54 Mb/s. Le 802.11n permet d'atteindre un débit réel supérieur à 100 Mb/s. Il est capable de fonctionner à 2,4 GHz ou à 5 GHz et est compatible avec le 802.11b/g et le 802.11a. Malheureusement, la plupart des équipements 802.11n disponibles aujourd'hui n'utilisent que la bande de fréquences de 2,4 GHz (et ne sont donc pas compatibles avec le 802.11a).

Aujourd'hui la variante du WiFi de la loin la plus utilisée est le 802.11g. Elle devrait être rapidement rattrapée par le 802.11n.

Variante	Débit Max.	Fréquence	Canaux	Modulation radio
802.11[a]	2 Mb/s	2,4 GHz	3	FHSS ou DSSS
802.11a	54 Mb/s	5 GHz	19	OFDM
802.11b	11 Mb/s	2,4 GHz	3	DSSS ou HR-DSSS
802.11g	54 Mb/s	2,4 GHz	3	DSSS ou HR-DSSS ou OFDM
802.11n	> 100 Mb/s	2,4 GHz ou 5 GHz	3 ou 19	DSSS ou HR-DSSS ou OFDM avec MIMO

a. Le 802.11 « tout court » désigne ici la première version du standard, parue en 1997.

Le fait que le WiFi soit conçu à l'origine pour réaliser des WLAN ne l'empêche pas d'être également utilisable dans d'autres contextes. Par exemple, une myriade de produits, tels que des agendas électroniques (organiseurs) ou *Personal Data Assistant* (PDA), des imprimantes, des écrans d'ordinateurs, des magnétoscopes ou encore des chaînes Hi-Fi, sont maintenant pourvus de connexions WiFi leur permettant d'être reliés entre eux sans le moindre fil. Dans ce cas, le WiFi est employé pour réaliser un WPAN. À l'inverse, de nombreuses collectivités locales n'ayant pas accès au haut débit (l'ADSL n'étant pas encore disponible partout) se tournent vers le WiFi pour couvrir toute une commune voire plusieurs communes avec un même réseau sans fil. On peut alors parler de *Wireless MAN* (WMAN).

Pour finir, des sociétés déploient actuellement des réseaux WiFi, appelés des *hotspots*[1], qui permettent à n'importe qui de se connecter à Internet sans fil un peu partout en France et dans le monde entier. On voit donc apparaître actuellement

1. *Hotspot* signifie « point chaud » en anglais.

ce que l'on pourrait appeler des WWAN (*Wireless Wide Area Networks*) basés sur la technologie WiFi (la technologie WiFi elle-même ne transporte cependant les données que sur de faibles distances). Nous y reviendrons dans les paragraphes suivants.

1.2.6 Les standards de l'IEEE

Comme nous l'avons vu, les produits WiFi reposent sur les protocoles WLAN publiés à partir de 1997 par l'IEEE sous le nom de 802.11. L'IEEE est l'un des principaux instituts américains de standardisation des technologies de communications. Il est issu de la fusion en 1963 entre l'*Institute of Radio Engineers* (IRE) et l'*American Institute of Electrical Engineers* (AIEE) dont les origines remontent à la fin du XIX^{e} siècle !

De nombreux standards de l'IEEE ont été ensuite ratifiés par l'ISO, ce qui leur confère une dimension mondiale. C'est le cas en particulier du standard Ethernet (802.3), et du WiFi (802.11). Le standard ISO correspondant au 802.11 est l'ISO/IEC 8802-11.

L'équivalent européen de l'IEEE est l'*European Telecommunications Standards Institute* (ETSI) qui propose sa propre technologie de réseau sans fil, le *High Performance Radio Local Area Network* (HiperLAN). Elle est toutefois beaucoup moins répandue aujourd'hui que le WiFi.

L'IEEE est composé d'un certain nombre de comités, eux-mêmes subdivisés en groupes de travail. Les comités sont tout simplement numérotés. Ainsi, le comité chargé des réseaux LAN et MAN correspond au numéro 802. Au sein de ce comité, les groupes de travail sont eux-mêmes numérotés et celui qui est chargé de standardiser les réseaux locaux sans fil porte le numéro 11. On le note donc 802.11 et il a donné son nom à la technologie. Avant le WiFi, le comité 802 avait déjà défini une foule de standards pour les réseaux, dont le plus connu et le plus répandu aujourd'hui est l'Ethernet (802.3), comme nous l'avons vu plus haut, qui permet de réaliser des réseaux locaux grâce à des câbles réseaux en cuivre ou en fibre optique. Voici quelques-uns des plus importants groupes de travail du comité 802 :

- **802.3** : LAN, standard dérivé d'Ethernet, initialement standardisé par les sociétés DEC, Intel et Xerox ;
- **802.5** : LAN, standard dérivé du Token Ring d'IBM ;
- **802.11** : WLAN, le WiFi ;
- **802.15** : WPAN, plusieurs standards, dont un dérivé de Bluetooth ;
- **802.16** : WMAN, le standard 802.16, à la base du WiMAX[1].

Maintenant que nous avons apporté toutes ces précisions sur l'origine du WiFi, voyons quelles en sont les principales applications.

1. Contrairement à une idée reçue, le WiMAX n'est pas une nouvelle version du WiFi : malgré quelques similitudes, il s'agit d'un tout autre protocole, conçu pour les WMAN et non les WLAN.

1.3 LES APPLICATIONS DU WIFI

1.3.1 L'extension du réseau d'entreprise

Bien que l'on trouve une multitude d'applications à la technologie WiFi, il est clair que sa première cible est le réseau d'entreprise. Comme nous l'avons vu, le WiFi a été conçu pour être une version sans fil d'Ethernet et ce dernier se retrouve dans presque toutes les entreprises. Dans la grande majorité des cas, une entreprise qui décide de s'équiper d'un réseau WiFi possède déjà un réseau filaire Ethernet. Il s'agit donc en règle générale de bâtir une extension sans fil pour un réseau filaire existant.

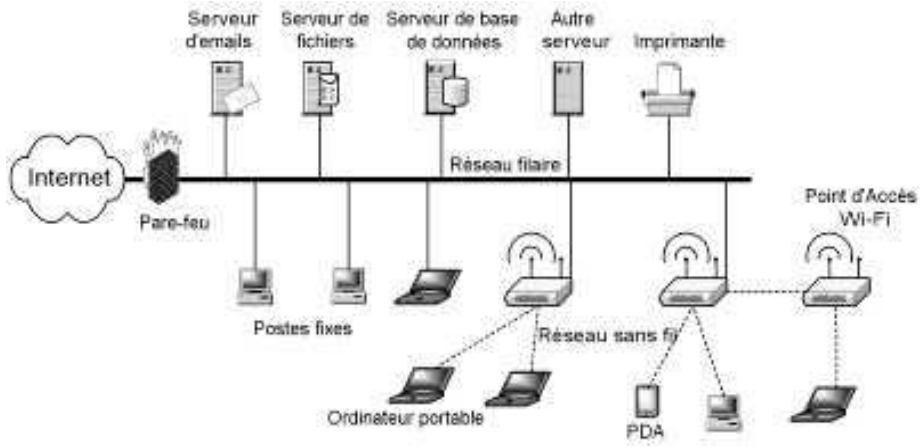


Figure 1.6 — Extension d'un réseau filaire grâce au WiFi.

Ceci pose un certain nombre de problèmes dont le plus évident est la sécurité. En effet, connecter une borne WiFi à un réseau d'entreprise sans se soucier de la sécurité signifie donner accès à toutes les ressources de l'entreprise au premier venu.

1.3.2 Le WiFi à domicile

Le WiFi a atteint le grand public et de plus en plus de particuliers s'équipent en WiFi pour construire un réseau familial. Le but est le plus souvent de permettre la connexion à Internet depuis n'importe quel endroit du domicile, ainsi que de partager cette connexion entre les différents membres de la famille. Le plus souvent, une seule borne WiFi suffit à couvrir un domicile de moins de 100 m^2. En outre, la plupart des Fournisseurs d'accès à Internet (FAI) proposent l'option WiFi depuis 2005 : le modem/routeur ADSL (la « *box* ») sert alors également de point d'accès WiFi.

L'autre motivation peut être de relier entre eux des équipements, tels que des écrans ou des imprimantes sans fil. Le WiFi empiète alors sur le domaine de prédilection de la technologie Bluetooth qui a été conçue pour un tel usage.

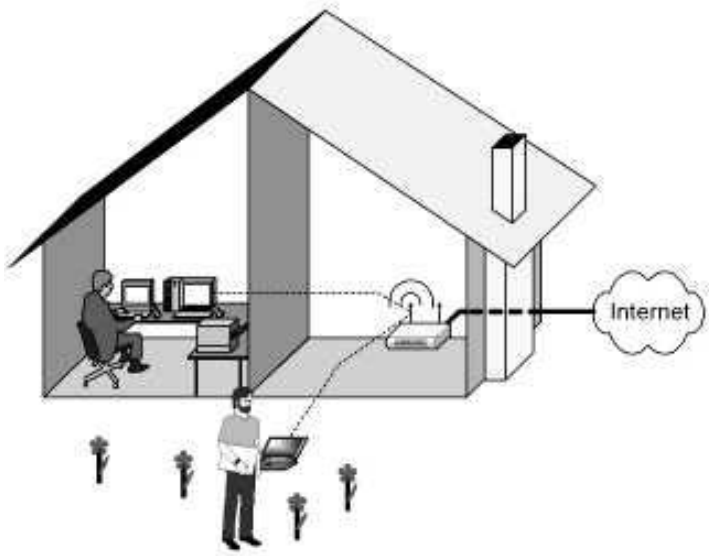


Figure 1.7 — Le WiFi à domicile : mobilité et partage de la connexion à Internet.

1.3.3 Les hotspots

Points d'accès sans fil à Internet

Un *hotspot* est un point d'accès sans fil à Internet (ou plus généralement à des services web). Il s'apparente donc à un cybercafé, à ceci près que le client utilise pour se connecter son propre ordinateur équipé de la technologie WiFi (ou son « *smartphone* » compatible WiFi, comme l'iPhone par exemple). Ceci lui permet de conserver, d'un *hotspot* à un autre, le même environnement de travail : le sien. On trouve des *hotspots* dans de nombreux sites où transitent des hommes d'affaires équipés d'ordinateurs portables : des aéroports, des gares, des hôtels, des centres de conférence, mais aussi des cafés, des restaurants, des universités et plus généralement presque tout type de lieu public. On peut également parfois les trouver dans des salles d'attente ou de réunion au sein de certaines entreprises soucieuses de fournir à leurs clients ou fournisseurs de passage un lien à Internet accessible et indépendant de leur propre réseau.

Les *hotspots* ont vu le jour dès l'an 2000, d'abord aux États-Unis, puis de façon virale un peu partout sur la planète et en particulier en Asie du Sud-Est où on les compte par milliers. Aux États-Unis, la chaîne de cafés Starbucks a fait sensation lorsqu'elle a équipé de *hotspots* l'ensemble de ses cafés. En France, les *hotspots* n'ont commencé à apparaître que fin 2002, lorsque la législation l'a permis. La société Wifirst (anciennement connue sous le nom de Wifix) a été la première à déployer des *hotspots* sur le territoire français (fig. 1.8). Très vite, elle a été rejointe par une multitude d'autres start-ups, telles que Wifispot, HotCafé ou encore Météor Networks, puis par de gros acteurs tels qu'Orange, SFR, Aéroports De Paris (ADP) Télécom, ou encore Swisscom et British Telecom. Ces opérateurs télécoms d'un nouveau genre

sont appelés les *Wireless Internet Service Providers* (WISP) c'est-à-dire Fournisseurs d'Accès à Internet (FAI) sans fil.

L'itinérance (ou roaming)

Avec l'apparition rapide de nombreux WISP indépendants, on a assisté à un morcellement important des réseaux de *hotspots*. En clair, quand on achetait un coupon de connexion ou un abonnement auprès d'un WISP donné, on n'avait en général accès qu'au réseau de ce WISP, c'est-à-dire le plus souvent à quelques dizaines ou centaines de *hotspots*. C'est pour résoudre ce problème que les WISP signent des accords d'itinérance (ou *roaming*) permettant aux abonnés d'un fournisseur donné de pouvoir « surfer » sur le réseau d'un autre fournisseur.

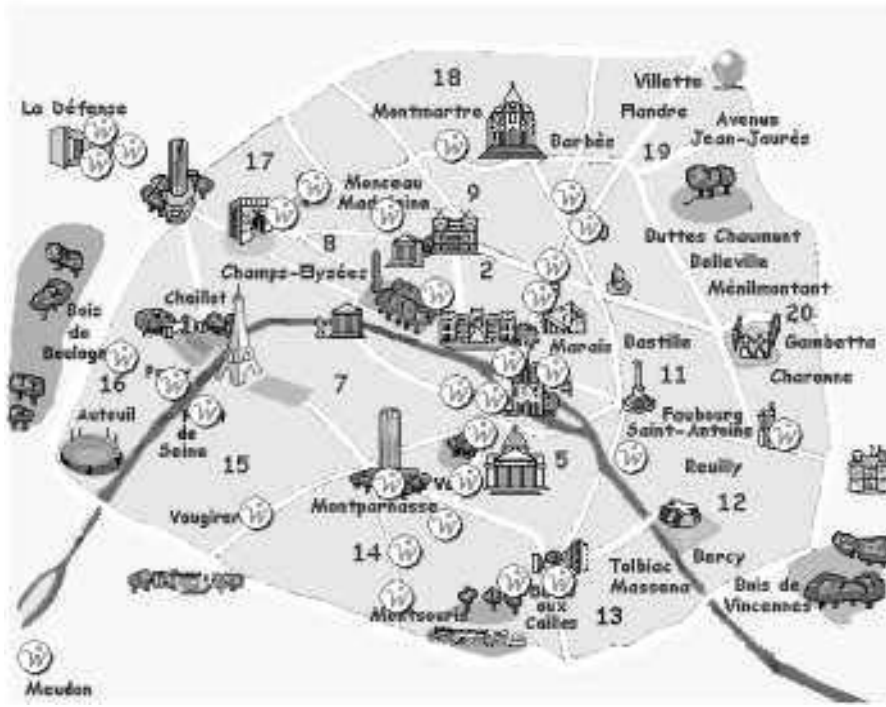


Figure 1.8 — Exemple de déploiement de *hotspots* d'un WISP à Paris.

Les trois opérateurs mobiles français, Orange, SFR et Bouygues, qui ont déployé le plus de *hotspots* à ce jour, ont ainsi créé une association appelée *Wireless Link* (c'est-à-dire « lien sans fil », noté W-Link) pour définir les modalités d'interopérabilité entre leurs réseaux. D'autres WISP les ont rejoints et si l'on rajoute à cela que de nombreux petits WISP disparaissent ou se font racheter, on peut penser que le morcellement des réseaux de *hotspots* va tendre à s'atténuer. À terme, on pourra peut-être se connecter à n'importe quel *hotspot* en France en ne payant qu'un seul abonnement auprès du WISP de son choix, voire même directement sur sa facture téléphonique si l'on passe par l'un des opérateurs mobiles.

Certains WISP ont déjà déployé un important réseau international par le biais des accords de *roaming*. C'est le cas des WISP Boingo et FatPort, par exemple. D'autres WISP n'ont en réalité jamais déployé eux-mêmes de *hotspots*, mais ont en revanche signé de nombreux accords de *roaming* à l'échelle internationale. On parle alors de « WISP virtuels ». On peut citer, parmi les plus importants, les sociétés GRIC Communications, iPass ou RoamPoint, par exemple. Est-il envisageable d'imaginer à terme un réseau mondial unifié ? Il est bien sûr encore trop tôt pour l'affirmer.

Enfin, une initiative originale mérite d'être mentionnée : la société Naxos, filiale de la RATP, a déployé un réseau WiFi dans de nombreuses stations de métro de Paris. Ce réseau couvre l'extérieur des stations de métro et permet donc de se connecter dans la rue ou à la terrasse des cafés voisins. L'originalité de ce projet, dénommé Wixos, réside dans le fait que Naxos a simplement déployé l'infrastructure WiFi, mais qu'elle laisse la gestion des clients et du paiement aux WISP partenaires de ce projet.

Les « box » deviennent des hotspots

Certains Fournisseurs d'Accès à Internet ont ouvert les « box » de leurs abonnés, les transformant en autant de hotspots. Un abonné de Free peut ainsi se connecter en WiFi à n'importe quelle Freebox pour laquelle cette option a été activée. Il n'a bien évidemment accès qu'à Internet, et non au réseau de l'abonné dont il emprunte la connexion. De même chez Neuf-SFR : l'option y est même activée par défaut.

Le nombre d'abonnés de ces FAI étant très important, lorsque l'on est en ville, on ne se trouve jamais très loin d'une zone couverte par une « box ». Le WiFi est donc déjà presque partout en ville.

Une couverture totale ?

On peut comparer ce phénomène de *hotspots* à ce qui s'est passé pour la téléphonie mobile : dans un premier temps, seuls quelques sites étaient couverts, puis les grandes villes ont été progressivement couvertes, puis les autoroutes, les petites villes et enfin presque tout le territoire. Si le développement des *hotspots* se poursuit au rythme actuel, il sera possible d'ici quelques années de se connecter à haut débit à Internet partout sur le territoire et même dans de nombreux pays grâce à la technologie WiFi.

Autres technologies

Des technologies concurrentes conçues spécialement pour la cible WMAN et WWAN, certaines plus résistantes aux obstacles et mieux adaptées aux couvertures radio de grande envergure que le WiFi, se battent pour dominer le marché. C'est le cas par exemple de la 2G (GPRS), de la 2,5G (EDGE), de la 3G (l'UMTS), la 3G+ (HSDPA), ou encore de la 4G (Wimax, LTE). Nous y reviendrons au § 1.4.

Et votre entreprise ?

Aujourd'hui, la majorité des ordinateurs portables professionnels sur le marché est équipée de la technologie WiFi. Si les employés de votre entreprise possèdent des ordinateurs portables récents, il est fort probable qu'ils soient d'ores et déjà « Wifisés ».

Figure 1.9 — Exemple d'interface de connexion à Internet et de gestion de compte.

Si vous installez un réseau WiFi dans votre entreprise, vous devrez équiper les ordinateurs les plus anciens d'adpateurs WiFi. Vos collaborateurs prendront l'habitude de se connecter sans fil. Tous les employés pourront alors se connecter à Internet sur n'importe quel *hotspot* WiFi en France ou à l'étranger. Ils pourront télécharger leurs e-mails au cours de leurs trajets, surfer sur Internet, se connecter à votre entreprise à distance *via* un Réseau Privé Virtuel (RPV), également appelé *Virtual Private Network* (VPN), etc. Bref, ils pourront rester productifs pendant leurs déplacements. C'est une des raisons de passer au WiFi dans votre entreprise.

Il peut également être intéressant de faire appel à un WISP pour mettre en œuvre un *hotspot* dans vos locaux, à l'usage de vos visiteurs, clients ou fournisseurs. Outre le service pour le visiteur et l'image moderne que cela pourra donner à votre société, ceci permettra d'améliorer la sécurité de votre réseau d'entreprise en évitant que des visiteurs ne passent par celui-ci pour se connecter à Internet. Vous pouvez bien sûr décider de mettre en œuvre ce *hotspot* par vous-même et ce livre peut vous aider à le faire.

1.3.4 Le WiFi communautaire

La technologie WiFi doit une partie de son succès aux initiatives d'associations telles que Paris sans fil (anciennement WiFi France) ou WiFi Montauban. Ces associations regroupent des passionnés du sans fil qui ont eu l'idée de conjuguer leurs efforts pour

tenter d'obtenir une couverture WiFi importante sur des sites de plus ou moins grande envergure. L'avantage de ces réseaux sur les *hotspots* classiques est leur gratuité totale !

Chaque membre dispose chez lui d'un petit réseau sans fil, ouvert à tous. Certaines associations ne font que fournir la liste des sites où l'on peut se connecter ainsi gratuitement, d'autres vont plus loin et relient entre eux les points d'accès, ce maillage permettant ainsi de partager les connexions à Internet. Ceci est particulièrement intéressant pour les habitants de communes où l'ADSL n'est pas disponible : ainsi, une seule connexion à Internet par satellite (assez coûteuse) peut être distribuée sur toute une commune grâce à un maillage serré de points d'accès WiFi (fig. 1.10).

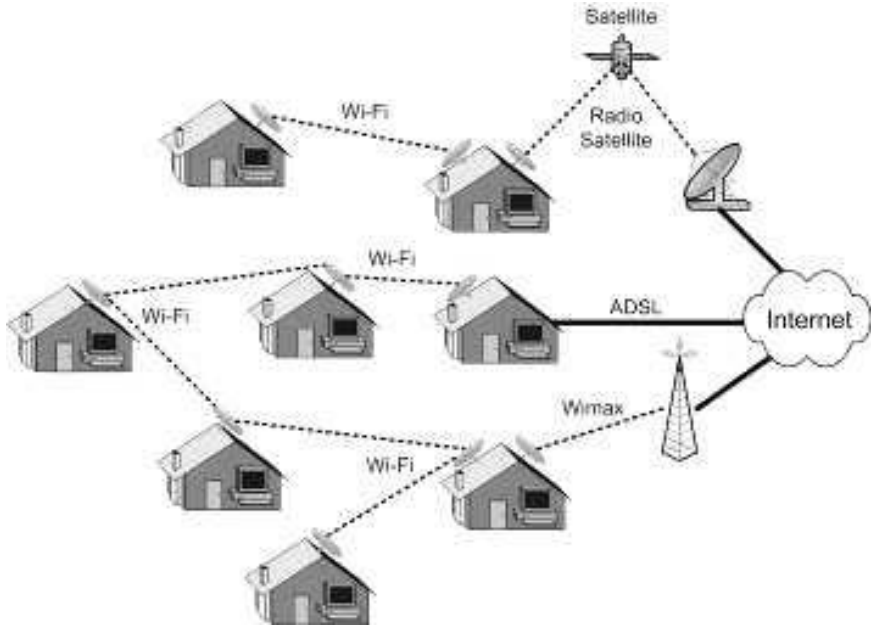


Figure 1.10 — Le WiFi communautaire et les différents types de connexion à Internet.

L'une des principales inquiétudes concernant ce modèle est sa légalité : en effet, en France, le propriétaire d'une connexion à Internet en est responsable. Si le réseau communautaire est ouvert à tous, sans contrôle d'identité, alors une personne mal intentionnée peut parfaitement abuser de la connexion à Internet, dans l'anonymat le plus complet. Elle pourra alors envoyer des milliers d'e-mails non sollicités (le *spam*), émettre des propos racistes ou diffamatoires, inciter à la violence ou encore échanger des fichiers illégaux (images ou vidéos illégales, produits commerciaux...). Dans ce cas, le propriétaire de la connexion à Internet peut être mis en cause pour ne pas en avoir protégé l'accès.

> Le propriétaire d'une connexion à Internet peut voir sa responsabilité engagée en cas d'abus : il ne doit donc pas laisser cette connexion libre d'accès pour des utilisateurs anonymes.

1.3.5 Le point à point

Avec le WiFi, il est possible de construire de simples liens sans fil, d'un point à un autre, à haut débit. Ceci est utile pour relier entre eux deux sites difficilement joignables par voie filaire, comme deux bâtiments d'une entreprise. La distance maximale entre les deux bâtiments dépend du débit que l'on souhaite garantir (plus la distance sera grande, plus le débit sera faible) et de la bande de fréquence choisie, mais on peut atteindre plusieurs mégabits par seconde jusqu'à 2 à 3 kilomètres en vision directe, c'est-à-dire sans obstacle sur l'axe ou proche de l'axe entre l'émetteur et le récepteur.

Il existe depuis longtemps des solutions de point à point basées sur d'autres technologies, dont le laser et les Faisceaux hertziens (FH). Toutefois, le WiFi a deux atouts :

- son coût très modeste : on peut réaliser un point à point de quelques centaines de mètres pour moins de 500 euros de matériel ;
- l'absence de licence : à condition de respecter les limites légales de puissance[1], le WiFi ne requiert pas de licence en France, alors qu'avec de nombreuses technologies concurrentes, il est nécessaire de faire une demande auprès de l'ARCEP et de payer tous les mois un montant, parfois important. Toutefois, la contrepartie de cette absence de licence est que rien n'interdit à votre voisin d'émettre sur vos fréquences et de gêner ainsi votre communication !

Nous étudierons en détail comment réaliser un point à point performant au cours du chapitre 5.

1.3.6 Le WiFi dans l'industrie

Une des preuves de la maturité du WiFi est le fait qu'on l'utilise pour faire davantage que de simples réseaux : l'industrie emploie de plus en plus d'applications variées qui reposent sur le WiFi. En voici quelques-unes des plus significatives.

Les inventaires

Des PDA, Smartphones ou Tablet PC sont équipés d'une connexion WiFi et permettent ainsi aux employés de réaliser des inventaires qui sont enregistrés en temps réel dans la base de données de l'entreprise. Ceci peut être utile pour les inventaires d'une grande surface, par exemple, pour gagner du temps. On trouve également cet usage du WiFi pour les loueurs de voitures, qui peuvent ainsi saisir directement à partir du parking les voitures qui partent et qui rentrent. Les aéroports de Paris utilisent également le WiFi pour enregistrer les bagages avant de les charger dans les avions. Ceci est un point crucial dans leur politique de sécurité car on doit toujours s'assurer que les bagages et leurs propriétaires sont bien dans le même avion.

1. Voir les tableaux synthétiques sur la législation au chapitre 11.

Le positionnement

Des logiciels installés sur des PDA équipés en WiFi permettent, en mesurant la puissance du signal radio provenant des différentes antennes WiFi voisines, de positionner avec une relative précision (moins de 2 mètres) le porteur du PDA, moyennant un étalonnage initial assez simple. Ceci peut être mis à profit dans les inventaires, bien entendu, mais également pour offrir à des clients un service localisé. Par exemple, un musée peut mettre ceci à profit pour offrir à ses visiteurs des informations sur les œuvres situées à leur proximité. Le visiteur n'a rien d'autre à faire que de se promener dans le musée muni de son PDA, prêté par le musée pour la durée de la visite.

La voix

L'une des grandes promesses du WiFi est sa capacité à gérer les communications audionumériques grâce aux technologies de voix sur IP (*Voice over Internet Protocol*, VoIP). Lorsque la VoIP est réalisée sur un réseau sans fil, on parle parfois de VoWIP (le « W » vient de *Wireless*), mais la technologie est absolument identique. Déjà, des sociétés proposent des téléphones VoWIP, reliés à votre réseau grâce au WiFi.

Bien que les téléphones en question soient encore pour l'instant assez volumineux et d'une autonomie limitée, leur avantage majeur est que le coût des communications est extrêmement faible. Pour joindre un autre téléphone VoIP, le coût est souvent nul. Vous pouvez aisément transformer votre ordinateur ou PDA en téléphone VoIP en installant un logiciel tel que Skype sur votre ordinateur. Il vous suffira de brancher un micro et un écouteur sur votre poste pour pouvoir en profiter. Ce type de logiciels permet de téléphoner gratuitement à un autre utilisateur possédant le même logiciel. Dans le cas de Skype, il est également possible de téléphoner vers un poste téléphonique classique, moyennant paiement.

La qualité du son est tout à fait comparable à la téléphonie fixe classique si votre bande passante est importante et réactive. Toutefois, afin d'éviter des interruptions dans la voix ou un temps de latence trop important, il sera sans doute nécessaire de mettre en œuvre une politique de qualité de service *Quality of Service*, QoS) pour garantir qu'une part de la bande passante soit réservée à vos communications téléphoniques. Ceci est d'autant plus vrai si vous vous connectez à Internet au travers de votre réseau WiFi, car selon le niveau de réception, le débit et le temps de latence peuvent varier de façon importante.

Le WiFi a été conçu pour les réseaux locaux et est donc parfaitement adapté à ce contexte, pour les réseaux familiaux ou professionnels.
Il connaît également de nombreuses autres applications comme les *hotspots,* les connexions de point à point ou la voix sur IP.

1.4 LES TECHNOLOGIES ALTERNATIVES

Une expression anglaise affirme que lorsqu'on possède un marteau, tout ressemble à un clou[1]. Nous venons de voir que le WiFi peut être utilisé dans presque tous les contextes, des plus petits réseaux aux plus grands. Toutefois, il ne faut pas perdre de vue qu'il est conçu pour les WLAN. Il existe d'autres technologies parfois mieux adaptées que le WiFi selon les contextes.

1.4.1 L'Ethernet

La première technologie concurrente du WiFi est évidemment... le filaire ! En effet, s'il s'agit par exemple de relier deux ou trois ordinateurs situés dans une même pièce, il est souvent moins coûteux en temps et en argent de connecter les ordinateurs à un simple routeur, à l'aide de quelques câbles réseaux, plutôt que de faire la même chose avec une connexion sans fil. En effet :

- la plupart des postes fixes sont vendus équipés d'un adaptateur réseau Ethernet, mais pas d'une carte WiFi ;
- la fiabilité et le débit d'un réseau filaire sont bien supérieurs au WiFi ;
- la sécurisation du réseau sera triviale en filaire puisqu'il n'y aura réellement rien à configurer, ou tout au plus un pare-feu (ou *firewall*) et un antivirus. Il sera plus complexe de sécuriser le réseau sans fil.

En outre, il est rare qu'une entreprise choisisse de reposer uniquement sur un réseau sans fil : la plupart du temps, le réseau sans fil n'est qu'une extension d'un réseau filaire préexistant. Passer au WiFi, ce n'est donc pas éliminer complètement les fils, mais le plus souvent offrir un moyen supplémentaire d'accéder aux données de l'entreprise. Il est donc essentiel de connaître les technologies filaires, même pour déployer du sans-fil.

Si vous devez relier deux sites entre eux, le WiFi ne sera peut-être pas capable d'assurer le débit et la fiabilité dont vous avez besoin. Une liaison Gigabit Ethernet filaire peut s'avérer être la meilleure solution.

1.4.2 Le CPL

La technologie CPL (Courant porteur en ligne) consiste à véhiculer des données par le biais de l'installation électrique d'un bâtiment. On la trouve notamment dans les produits respectant la norme HomePlug.

Le CPL est parfois mieux adapté que le WiFi. Par exemple, dans un bâtiment à plusieurs étages ou aux murs très épais, un seul point d'accès WiFi sera sans doute insuffisant, alors que le CPL passera par les fils électriques et ne craindra donc pas les murs.

1. *If the only tool you have is a hammer, you will see every problem as a nail.* Abraham Maslow.

Toutefois, le CPL n'a pas que des avantages :

- il ne permet pas une vraie mobilité : on reste relié à un câble ;
- certaines installations électriques laissent mal passer le CPL, en particulier au niveau des disjoncteurs et des tableaux électriques ;
- la sécurité des données n'est pas le point fort du CPL. Il est possible de crypter l'ensemble des communications, mais cela suppose que chaque équipement soit configuré avec un même mot de passe, ce qui n'est envisageable que sur de petits réseaux personnels.

Le CPL et le WiFi peuvent également être complémentaires : dans un réseau WiFi composé de plusieurs AP, le CPL peut permettre de relier les AP entre eux et d'éviter ainsi un câblage coûteux.

1.4.3 L'infrarouge et le laser

Communication à courte distance

La lumière infrarouge est utilisée depuis de nombreuses années pour la communication directe entre des équipements proches l'un de l'autre, tels que votre télécommande et votre télévision, par exemple.

Ces ondes ne sont pas capables de traverser les obstacles et la puissance du signal se dissipe rapidement : la portée est donc faible. À courte distance, le débit peut toutefois être assez élevé : l'organisme IrDA a développé une série de standards, dont le plus rapide à ce jour, le *Very Fast Infrared* (VFIR) permet d'atteindre un débit de 16 Mb/s. Il est donc parfaitement adapté pour les échanges de données entre deux terminaux, par exemple pour l'échange de cartes de visites entre deux smartphones, ou encore la copie de photographies à partir d'un appareil photo numérique vers un ordinateur. L'aspect directionnel et la faible portée du signal offrent une certaine sécurité contre les écoutes pirates. Les ondes infrarouges n'interfèrent absolument pas avec les ondes radio ce qui est appréciable dans un environnement électromagnétique « bruyant ».

L'infrarouge est souvent mieux adapté que le WiFi pour réaliser des WPAN, c'est-à-dire, comme nous l'avons vu, pour permettre les échanges entre périphériques situés à proximité les uns des autres. Notons que les standards de l'IrDA permettent aussi de réaliser de véritables WLAN, mais leur intérêt est très limité face au WiFi pour cet usage.

Point à point

En concentrant le signal en un faisceau cohérent, très étroit, à l'aide de diodes laser plutôt que de simples *Light-Emitting Diodes* (LED), il est possible de réaliser des liens de point à point sur plusieurs kilomètres, mais dans la pratique il vaut mieux se limiter à quelques dizaines de mètres seulement, car sinon la pluie et le brouillard couperont fréquemment la connexion.

Ici encore l'aspect directionnel du laser et le fait qu'il n'interfère pas avec la radio sont des avantages face au WiFi pour mettre en place une liaison point à point en milieu urbain saturé en ondes radios.

1.4.4 Le Bluetooth

Le Bluetooth est, avec l'infrarouge, l'une des principales technologies sans fil développées pour réaliser des WPAN. Cette technologie est mise en avant par le *Bluetooth Special Interest Group* (Bluetooth SIG) qui a publié la première version de la spécification Bluetooth en 1999.

La technologie Bluetooth utilise les ondes radios dans la bande de fréquence de 2,4 GHz, ce qui permet de traverser certains obstacles d'épaisseur modeste. On peut ainsi transférer des données au travers de murs, de poches ou de porte-documents, ce dont l'infrarouge est incapable. Il est important de noter que c'est la même bande de fréquences que celle utilisée par le 802.11b/g, ce qui peut poser des problèmes d'interférences entre les deux technologies.

Comme le WiFi, le Bluetooth connaît un succès considérable : il existe des souris Bluetooth, des écrans Bluetooth, des PDA Bluetooth, etc. La configuration d'un équipement Bluetooth est en général tout à fait triviale car le standard définit un mécanisme de détection automatique des services Bluetooth situés à proximité. Cette technologie est sans doute mieux adaptée aux WPAN que le WiFi, pour lesquels la configuration n'est pas toujours évidente. En outre, la consommation électrique, la taille et le prix des adaptateurs Bluetooth sont bien plus faibles que pour le WiFi. Mais bien qu'il soit possible de construire un réseau WLAN avec le Bluetooth, le WiFi reste généralement mieux adapté pour cet usage.

1.4.5 La « data mobile »

Nous avons vu que le WiFi peut permettre de se connecter à Internet, un peu n'importe où, grâce à des « *hotspots* ». C'est intéressant pour des connexions occasionnelles, mais si vous vous déplacez souvent et que vous avez besoin d'une connexion à Internet partout où vous vous trouvez, alors les offres de « data mobile » des opérateurs de téléphonie mobile sont sans doute la meilleure solution. Le coût sera peut être plus élevé que celui des *hotspots* WiFi (encore que cela dépende des *hotspots*), et le débit plus faible, mais vous aurez de bien meilleures chances de pouvoir vous connecter à Internet où que vous soyez.

Les solutions principales de « data mobile » en France sont :

- **Le *General Packet Radio Service* (GPRS)** : présent partout où la couverture mobile existe, il a malheureusement un débit faible (quelques dizaines de kb/s) et un coût élevé. On parle de téléphonie de seconde génération (2G).
- **L'*Enhanced Data rates for GSM Evolution* (EDGE)** : il a une couverture moins importante, mais un débit plus élevé. On parle parfois de « 2,5G ».
- **L'*Universal Mobile Telecommunications System* (UMTS)** : plus souvent appelé « 3G », il a une bonne couverture et un débit encore plus élevé (quelques centaines de kilobits par seconde).
- **Le *High Speed Downlink Packet Access* (HSDPA)** : il s'agit d'une amélioration de l'UMTS permettant d'atteindre un débit de plusieurs Mb/s. On le désigne généralement sous le nom commercial de « 3G+ ».

Quelle sera la technologie de quatrième génération (4G) ? Il y a actuellement deux prétendants : le WiMAX et le *Long Term Evolution* (LTE). Les deux permettront d'atteindre un débit de plus de 10 Mb/s. Le déploiement du WiMAX a commencé en 2006 en France, tandis que le LTE n'est pas attendu avant 2011. Toutefois, la réglementation française interdit pour l'instant aux opérateurs WiMAX de proposer à leurs clients un usage mobile : ils ne doivent proposer qu'un service de type Boucle locale radio (BLR), c'est-à-dire offrir un accès à Internet fixe, en installant une antenne chez le client. Le LTE a donc de fortes chances de devenir la technologie de la 4G en France.

On croit souvent que le WiMAX est une version améliorée du WiFi : il n'en est rien. Le Wimax est un label de qualité et d'interopérabilité délivré par le WiMAX Forum pour les produits respectant les normes IEEE 802.16 et ETSI HiperMAN. Le WiMAX s'attaque donc aux WMAN. Le WiFi est également un label de qualité et d'interopérabilité, mais il est délivré par la WiFi Alliance, pour les produits respectant la norme IEEE 802.11. Il vise les WLAN. Malgré un nom semblable et quelques similitudes techniques, il s'agit bien de technologies tout à fait distinctes.

1.4.6 Autres technologies

Il existe encore bien d'autres technologies radio, susceptibles d'être plus intéressantes que le WiFi dans certains contextes :

- **Le ZigBee**, technologie WPAN à faible portée, faible débit, faible consommation électrique et faible coût.
- **L'*Ultra Wideband* (UWB)**, c'est-à-dire « bande de fréquence ultra-large », technologie WPAN à faible portée et très haut débit.
- **Les Faisceaux hertziens (FH)** sont des connexions radio de point à point reposant sur des fréquences sous licence, avec des technologies variées. Ils permettent d'établir sur plusieurs kilomètres de distance un pont radio très fiable, car les fréquences radio sont réservées, contrairement au WiFi. Mais ils ont des inconvénients : le matériel est cher, il faut demander l'autorisation à l'ARCEP et lui payer ensuite une redevance annuelle.
- **Les variantes propriétaires du WiFi**, comme l'ancien « 802.11b+ » de Texas Instrument ou encore le « Super G » d'Atheros Communications, sont mises en œuvres dans certains équipements WiFi. Si l'émetteur et le récepteur sont tous deux compatibles, le débit peut être considérablement amélioré. Sinon, si l'un des équipements n'est pas compatible, la communication a lieu en WiFi standard.

Pour finir, notons que la technologie *High Performance LAN* (HiperLAN), technologie WLAN qui fut développée par l'ETSI, un organisme européen semblable à l'IEEE, a presque disparu, vaincue par le WiFi. De même, la technologie *Home Radio Frequency* (HomeRF), conçue par le *HomeRF Working Group* (HomeRF WG) dans le but d'étendre les capacités du standard *Digitally Enhanced Cordless Telephony* (DECT)

des téléphones sans fil, a également été écrasée par le succès du WiFi, en tout cas pour les usages de type WLAN.

1.4.7 La place du WiFi

Les paragraphes précédents ont rappelé que le WiFi a été conçu avant tout pour les réseaux locaux sans fil, les WLAN. Pour les autres usages, il a de sérieux concurrents. La figure 1.11 récapitule la place relative des différentes technologies selon deux axes : le débit et l'étendue du réseau.

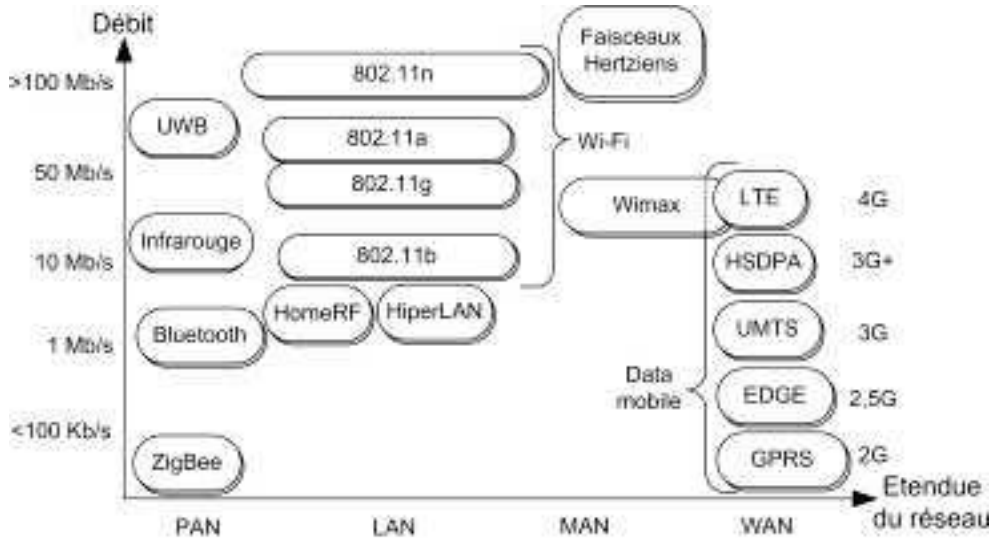


Figure 1.11 — La place du WiFi parmi les autres technologies sans-fil.

Résumé

Dans ce chapitre, nous avons commencé par un bref historique des ondes radio, et nous avons montré pourquoi les réseaux sans fil ne connaissent le succès que maintenant : l'apparition de standards a permis aux prix de chuter, les réglementations se sont homogénéisées, et les nouvelles technologies permettent des débits comparables aux réseaux filaires.

Nous avons rappelé les termes et concepts fondamentaux des réseaux : les couches de protocoles, le modèle OSI, et les principaux types de réseaux : PAN, LAN, MAN, WAN et leurs variantes sans fil, dont le WLAN (ou RLAN si la technologie est la radio).

Nous avons ensuite présenté les principales applications du WiFi : réseau d'entreprise, réseau familial, *hotspots*, réseau communautaire, connexion de point à point, inventaires, positionnement ou voix sur IP.

Cette élasticité du WiFi, c'est-à-dire sa capacité à s'adapter à des usages très variés, explique sans doute en grande partie son succès. Il ne faut cependant pas perdre de vue qu'il a été conçu pour réaliser des réseaux de type WLAN, particulièrement pour les entreprises : pour cet usage, il domine actuellement le marché ; pour les autres il a des concurrents très sérieux, comme nous l'avons vu.

Il est temps maintenant de s'attaquer au cœur de la bête : les rouages de la norme 802.11.

2

La norme 802.11 : couches physiques

Objectif

Dans ce chapitre et le suivant, vous apprendrez comment fonctionne le WiFi. Le but est de vous apporter une bonne compréhension technique de la norme 802.11. Bien sûr, on peut très bien déployer un réseau sans fil sans comprendre les mécanismes qui le mettent en œuvre, de même que l'on peut conduire une voiture sans comprendre le fonctionnement de son moteur. Toutefois, si vous prenez le temps de bien maîtriser les aspects les plus techniques du WiFi, vous pourrez plus facilement choisir le matériel le mieux adapté à vos besoins, optimiser votre réseau et résoudre certains problèmes qui pourraient survenir dans la vie de votre réseau sans fil (problèmes liés notamment aux interférences radio ou à des paramètres obscurs de votre matériel WiFi). Avoir une idée de ce qu'est une modulation radio constitue un élément de culture générale important dans le milieu des technologies sans fil. Le résumé en fin de chapitre vous sera utile si vous ne voulez pas vous encombrer de toutes les explications techniques.

2.1 UNE VUE D'ENSEMBLE

La toute première version du 802.11, publiée en 1997, s'appelait simplement 802.11. La dénomination portant maintenant à confusion (car on utilise maintenant ce nom pour désigner l'ensemble des protocoles de la série), on lit souvent le nom *802.11legacy*

pour désigner cette première version, ce qui signifie littéralement « 802.11hérité » ou encore « 802.11historique ».

2.1.1 Trois couches physiques

Le 802.11legacy définit trois couches physiques : l'une sur infrarouge et les deux autres sur les ondes radio de fréquences 2,4 GHz, avec un débit théorique de 1 ou 2 Mb/s.

La couche physique reposant sur l'infrarouge n'a jamais connu le succès, sans doute parce que de meilleurs produits, basés sur l'infrarouge et standardisés par l'IrDA, existaient déjà. Nous n'en parlerons donc pas davantage.

Sur les deux couches radio, l'une utilise la modulation radio de type DSSS et l'autre de type FHSS (voir le § 2.3, *Les modulations radio*). On les appelle donc simplement les couches 802.11 DSSS et 802.11 FHSS. La couche 802.11 DSSS a connu des améliorations (802.11b et 802.11g), alors que la couche 802.11 FHSS a plus ou moins été abandonnée.

2.1.2 Une couche MAC

En plus de ces trois couches physiques, le standard 802.11legacy définit la couche 2 du modèle OSI (la couche de liaison de données), ou plus exactement la partie basse de cette couche appelée la couche *Media Access Control* (MAC).

La couche MAC s'occupe de coordonner l'accès à la couche physique. Elle définit en particulier comment plusieurs périphériques devront partager le temps de parole sur les ondes radio, comment un périphérique doit se connecter (on dit « s'associer ») à un réseau sans fil et également comment sécuriser les données échangées. Nous y reviendrons au chapitre 3.

2.1.3 Les évolutions du 802.11

Au fil des années, des améliorations importantes ont été apportées au standard 802.11. Certaines concernent la couche physique, d'autres concernent la couche MAC. Ces améliorations sont simplement désignées par une lettre rajoutée au nom du standard, de façon simplement séquentielle (802.11a, 802.11b...). Les principales améliorations concernant les couches physiques sont :

- **802.11a** : fréquence radio à 5 GHz au lieu de 2,4 GHz, modulation radio de type OFDM (voir paragraphes suivants), débit maximal théorique de 54 Mb/s ;
- **802.11b** : fréquence radio à 2,4 GHz, modulation DSSS ou HR-DSSS, débit maximal théorique de 11 Mb/s ;
- **802.11g** : fréquence radio à 2,4 GHz, modulation DSSS, HR-DSSS ou OFDM, débit maximum théorique 54 Mb/s ;

- **802.11n** : devrait être ratifié en janvier 2010, mais des études (*draft*) du standard ont été publiées depuis 2006 et sont déjà utilisées aujourd'hui. Compatible avec le 802.11a et le 802.11b/g, il permet, grâce à de nombreuses améliorations techniques telles que le MIMO (cf. § 2.3.6) d'atteindre des débits très élevés (> 100 Mb/s réels).

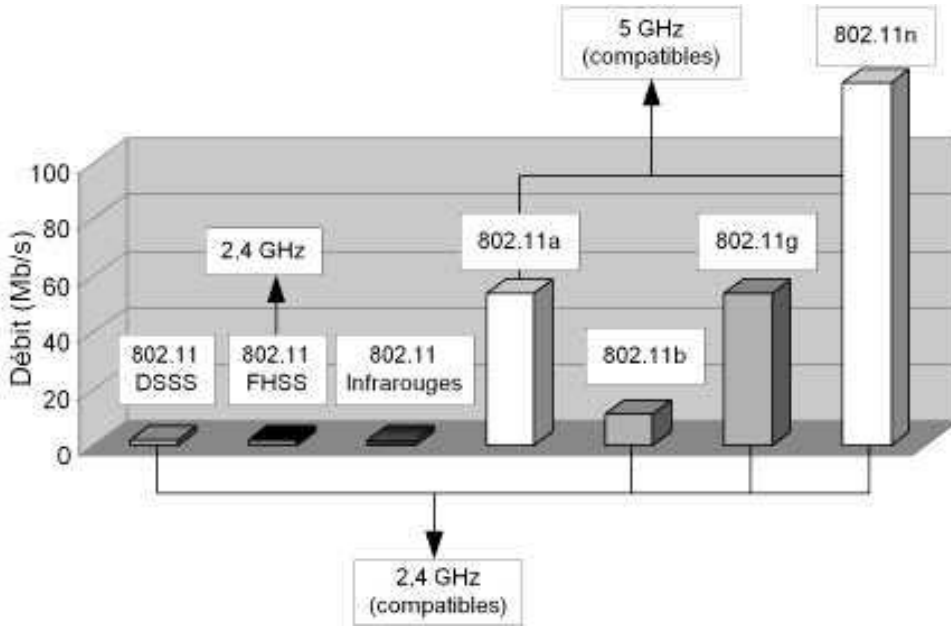


Figure 2.1 — Les couches physiques du WiFi : débit, fréquence et compatibilité.

Nous allons maintenant aborder plus en détail les différentes couches physiques du WiFi, en commençant par quelques rappels sur la radio, puis en détaillant les modulations radio les plus importantes.

2.2 QUELQUES RAPPELS SUR LES ONDES RADIO

2.2.1 Les grandeurs physiques des ondes

Les ondes radio, également appelées ondes hertziennes car elles furent découvertes par le physicien allemand Heinrich Hertz en 1888, sont des ondes électromagnétiques, c'est-à-dire des oscillations combinées d'un champ électrique et d'un champ magnétique. Les ondes radio, les infrarouges, la lumière visible, les ultraviolets, les rayons X ou encore les rayons gammas sont tous des exemples d'ondes électromagnétiques (fig. 1.2). Ces ondes transportent de l'énergie sans avoir besoin d'un quelconque support matériel (contrairement au son, par exemple) : autrement dit, elles peuvent se propager dans le vide.

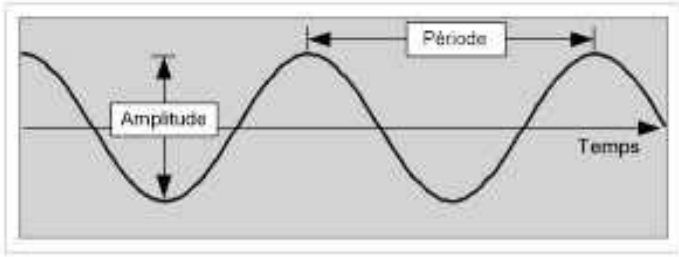


Figure 2.2 — Une onde et ses grandeurs physiques.

Comme toutes les oscillations, il est possible de caractériser une onde électromagnétique par quelques grandeurs essentielles :

- **La fréquence de l'onde** (notée υ) est le nombre d'oscillations par seconde, mesurée en hertz (Hz). Par exemple, les ondes radio du 802.11b oscillent environ 2,4 milliards de fois par seconde : la fréquence est donc égale à 2,4 GHz ! À titre de comparaison, la lumière visible se situe à des fréquences encore bien plus élevées : entre 530 térahertz (THz) pour le rouge (soit 530 000 GHz) et 750 THz pour le violet. Inversement, les ondes des stations de radio FM se situent environ à 100 mégahertz (MHz).
- **La période** (notée T) est la durée d'une oscillation complète. On la mesure bien sûr en secondes (s). Il s'agit simplement de l'inverse de la fréquence ($T = 1/\upsilon$). Encore pour le 802.11b, elle est donc environ égale à 0,42 nanoseconde (ns).
- **La vitesse de propagation** de l'onde dans l'espace : on parle de « célérité », notée c et mesurée en mètres par seconde (m/s). Dans le vide, elle est égale à la vitesse de la lumière : c = 299 792 458 m/s soit environ 300 000 km/s. Elle est moins élevée selon la nature du milieu traversé : environ 299 700 km/s dans l'air, par exemple et environ 230 000 km/s dans l'eau.
- **La longueur d'onde**, notée λ et mesurée en mètres (m), est la distance parcourue par l'onde pendant une oscillation. On la calcule facilement en multipliant la période de l'onde par sa vitesse ($\lambda = T * c$). Toujours pour le 802.11b, la longueur d'onde est donc environ égale à 12,6 centimètres (cm). La taille d'une antenne correspond souvent à un multiple de la longueur d'onde : la moitié ou le quart, en général.
- **L'amplitude** de l'onde électromagnétique est la « hauteur » de l'onde, si l'on prend l'analogie avec une vague d'eau. L'amplitude électrique se mesure en volts par mètre (V/m) et l'amplitude magnétique en teslas (T), les deux étant directement liées quand on parle d'ondes électromagnétiques. L'intensité est le carré de l'amplitude et elle détermine la puissance. Dans la pratique, avec le WiFi, on préfère utiliser directement la grandeur de puissance plutôt que de s'encombrer avec l'amplitude.
- **La puissance** de l'onde dépend de l'amplitude et de la fréquence. Elle se mesure en Watt (W). Les émetteurs WiFi émettent en général des ondes d'une puissance de l'ordre de 100 mW. On parle également en décibels de milliWatt, notés dBm

(et plus rarement en décibels de Watt, notés dBW). Voici les formules pour convertir d'une unité à l'autre :

$$Puissance_{dBm} = 10 \times \log\left(Puissance_{mW}\right)$$

et

$$Puissance_{mW} = 10^{\left(\frac{Puissance_{dBm}}{10}\right)}$$

Par exemple, un émetteur WiFi à 20 dBm est un émetteur à 100 mW.

- **La phase** de l'onde (notée φ) est la position de l'onde dans le temps (en degrés). Deux ondes de même fréquence sont « en phase » ($\Delta\varphi = 0°$) lorsqu'elles sont parfaitement synchrones, et « en opposition de phase » ($\Delta\varphi = 180°$) lorsque le maximum de l'une correspond au minimum de l'autre.

2.2.2 Les règles de la transmission radio

La théorie des ondes électromagnétiques est trop vaste et complexe pour la traiter ici en détail. Voici donc les principaux résultats qu'il faut retenir.

La portée du signal

Bien évidemment, plus la puissance est importante, plus la portée du signal est grande et plus les ondes traversent les obstacles. En deux mots, pour doubler la portée du signal, il faut quadrupler la puissance de l'émetteur. Pour vous en convaincre, imaginez qu'une ampoule soit placée au centre d'un abat-jour sphérique de rayon R (fig. 2.3). L'énergie lumineuse de l'ampoule est répartie de façon homogène sur l'ensemble de la surface de la sphère. Or, la surface d'une sphère se calcule par la formule suivante : $Surface = 4 \times \pi \times R^2$. Si l'on remplace notre abat-jour par un autre de rayon double, sa surface sera quatre fois plus grande, et donc quatre fois moins éclairée, si l'on ne change pas d'ampoule. Résultat : pour que l'abat-jour soit autant éclairé qu'auparavant, il faut utiliser une lampe quatre fois plus lumineuse.

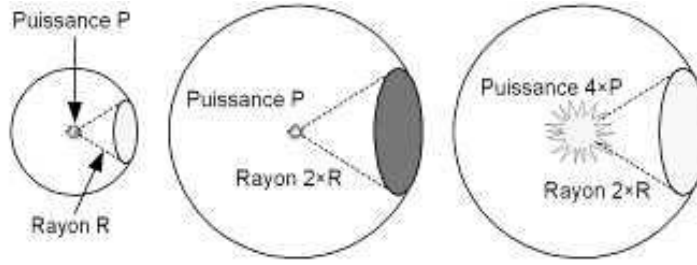


Figure 2.3 — La puissance d'émission et la portée du signal.

Quand on parle de « quadrupler la puissance » de l'émetteur, il s'agit de la puissance exprimée en Watt. Par exemple, un émetteur à 100 mW porte deux fois plus loin qu'un émetteur à 25 mW. Mais qu'en est-il des dBm ? Pour le savoir, il faut revenir à leur définition et voir ce qui se passe si l'on quadruple la puissance[1] :

$$\begin{aligned} QuadruplePuissance_{dBm} &= 10 \times \log(QuadruplePuissance_{mW}) \\ &= 10 \times \log(4 \times Puissance_{mW}) \\ &= 10 \times \log(4) + 10 \times \log(Puissance_{mW}) \\ &= 10 \times \log(4) + Puissance_{dBm} \end{aligned}$$

Lorsque l'on parle en dBm, « quadrupler la puissance » signifie simplement rajouter $10 \times \log(4) \approx 6{,}02$ dBm. Par exemple, un émetteur d'une puissance égale à 20 dBm est quatre fois plus puissant qu'un émetteur de 14 dBm et il porte donc deux fois plus loin.

> Pour doubler la portée du signal, il faut multiplier la puissance de l'émetteur par quatre. Ceci correspond à une augmentation de 6 dBm.

Par ailleurs, les basses fréquences ont une meilleure portée et traversent mieux les obstacles[2]. À puissance d'émission égale, les ondes radio à 2,4 GHz portent environ deux fois plus loin que les ondes à 5 GHz. Toutefois, la législation autorise des puissances de 200 à 1000 mW pour le 5 GHz alors que la limite n'est que de 100 mW pour le 2,4 GHz, ce qui compense la différence.

La sensibilité du récepteur est également très importante : certaines cartes 802.11b ont un *seuil de sensibilité* de −88 dBm pour un débit de 1 Mb/s (ou −80 dBm pour 11 Mb/s). Cela signifie qu'elles seront capables de maintenir une connexion WiFi à 1 Mb/s même si le signal perçu n'a qu'une puissance de −88 dBm. Toutefois, il existe également des cartes de meilleure qualité avec une sensibilité de −94 dBm ou mieux encore. Cette différence, d'apparence anodine, est en réalité énorme : 6 dBm, c'est un rapport de puissance du simple au quadruple, comme nous venons de le voir ! La portée de ces cartes sera donc deux fois supérieure aux premières, en tout cas dans un environnement peu bruyant.

Dans un environnement très bruyant, la sensibilité ne joue plus autant, mais est relayée par la *tolérance au bruit*. Par exemple, pour certaines cartes 802.11b, le rapport signal/bruit doit être au minimum de 4 dB pour qu'une communication à 1 Mb/s puisse être soutenue. D'autres cartes auront des valeurs différentes et il est donc important de vérifier ces paramètres avant l'achat.

1. Pour comprendre le raisonnement, il faut savoir que $\log(a \times b) = \log(a) + \log(b)$.
2. De même, lorsque votre voisin met de la musique, vous entendez surtout les graves (basses fréquences).

Bruit, interférences et multipath

Le Rapport signal/bruit (RSB)[1] est crucial pour bénéficier d'une bonne qualité de communication. Il s'exprime en décibels (dB) et correspond simplement à la différence entre la puissance du signal reçu et la puissance du bruit (exprimés en dBm) :

$$RSB = Puissance\ du\ signal\ reçu_{dBm} - Puissance\ du\ bruit_{dBm}$$

Plus le RSB est important, plus la réception est bonne et permet des débits importants. Par exemple, si le bruit est de −100 dBm et que le signal reçu est de −65 dBm, alors le RSB est de +35 dB.

Parmi les sources de bruit, on trouve bien sûr les réseaux sans fil et tous les équipements radio situés à proximité, mais il y a également un bruit ambiant lié à l'activité humaine (industrielle, militaire, radios, télévision, antennes de téléphonie mobile...) et le bruit électromagnétique naturel. La puissance du bruit naturel est en général de l'ordre de −100 dBm pour les fréquences du WiFi.

En outre, les interférences peuvent également provenir du signal lui-même : pour parvenir au récepteur, le signal peut parfois parcourir plusieurs chemins (on parle de *multipath*) du fait de multiples réflexions : par exemple, une partie du signal peut aller en ligne droite vers le récepteur et une autre peut rebondir sur un mur avant d'atteindre sa destination (fig. 2.4). Selon le chemin parcouru, le signal ne va pas mettre le même temps pour parvenir à destination. Ce phénomène provoquera, au niveau du récepteur, à la fois des interférences radio (donc du bruit) mais aussi un signal étalé dans le temps : des symboles[2] peuvent alors se superposer aux symboles suivants, ce qui provoque alors des erreurs de transmission. Dans ce cas, on parle d'interférence inter-symboles (*Inter-Symbol Interference*, ISI). C'est un peu la même chose que d'essayer de parler au téléphone lorsqu'il y a beaucoup d'écho : on entend le mot précédent en même temps qu'on prononce le suivant et il est assez difficile de communiquer dans ces conditions.

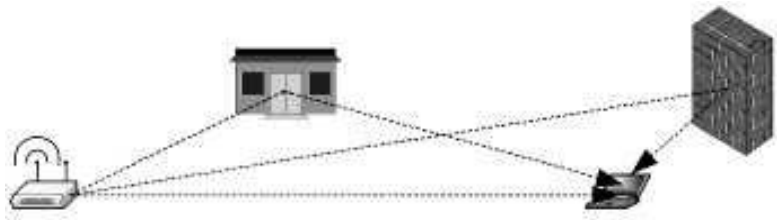


Figure 2.4 — Les chemins multiples (multipath).

Les récepteurs WiFi ont une plus ou moins grande tolérance aux délais dus aux réflexions : en règle générale, pour un débit de 1 Mb/s, ce délai est de l'ordre de

1. *Signal to Noise Ratio* (SNR ou S/N).

2. Un paquet de données est transmis, au niveau physique, par une séquence (ou « trame ») de symboles, chaque symbole pouvant représenter un ou plusieurs bits d'information. Nous y reviendrons dans les paragraphes suivants.

500 ns. Étant donné qu'une onde radio se déplace dans l'air environ à la vitesse de la lumière, elle parcourt environ 150 mètres en 500 ns. Ainsi, pour rester dans la limite de tolérance d'une carte acceptant des délais de 500 ns, il ne faut pas que les différents chemins pour le signal aient des longueurs différentes de plus de 150 mètres. Concrètement, c'est rarement un problème, surtout en entreprise. En revanche, pour un débit de 11 Mb/s, le délai toléré par la plupart des cartes 802.11b descend à 65 ns environ. Cela signifie des différences de parcours de 20 mètres environ. Dans un hall ou un entrepôt, cela peut devenir un problème.

Il faut bien distinguer la portée en vision directe (*Line of Sight* ou LOS) de la portée en intérieur ou avec obstacles (Non-LOS ou NLOS). Nous verrons que certaines modulations permettent d'optimiser la tolérance aux obstacles, mais pénalisent la portée en vision directe.

Pour finir, plus un signal est étalé sur un spectre de fréquences large, plus le risque de multipath est important, car les ondes ne se réfléchissent pas de la même façon sur les obstacles selon leur fréquence. Un signal étalé aura donc tendance à se réfléchir dans toutes les directions, contrairement à un signal utilisant une étroite bande de fréquences.

Le débit

Pour obtenir un bon débit, il est nécessaire d'avoir un bon rapport signal/bruit. Puisque le RSB diminue lorsqu'on s'écarte de l'émetteur, on en déduit que le débit diminue avec la distance (fig. 2.5). De fait, avec un émetteur 802.11g à 15 dBm et un bon récepteur, on peut en théorie, en conditions idéales (pas de bruit ni d'obstacles), obtenir un débit de 11 Mb/s jusqu'à 100 mètres environ, mais au-delà le débit tombera à 5,5 Mb/s, puis à 2 Mb/s et enfin à 1 Mb/s jusqu'à plus de 300 m. Dans la pratique, la portée est souvent plus faible (de l'ordre de la moitié ou du tiers selon les conditions). En outre, le débit réel est souvent deux ou trois fois plus faible que le débit théorique.

Par ailleurs, le débit maximal que l'on peut atteindre est proportionnel à la largeur de la bande de fréquence utilisée. On peut comparer ce phénomène au trafic automobile sur une autoroute : le débit maximal est plus important sur une autoroute à trois voies que sur une autoroute à deux voies.

Or, plus on se situe sur des fréquences élevées, plus on a « de la place » pour exploiter des bandes de fréquences larges[1], donc plus le débit peut être important. Cependant, dans le cas du WiFi, les canaux de communication définis pour le 2,4 GHz ont une largeur de 22 MHz alors que les canaux du 5 GHz ont une largeur de 20 MHz (voir à la fin de ce chapitre). Le débit maximal que l'on peut théoriquement atteindre est donc plus ou moins identique dans les deux cas. Ceci explique pourquoi le 802.11a et le 802.11g offrent tous les deux le même débit maximal, malgré le fait que le 802.11a exploite des fréquences plus élevées que le 802.11g. Cependant, il y a plus de canaux

1. Par exemple, si le canal de communication est centré sur la fréquence 100 kHz, sa largeur ne peut manifestement pas être supérieure à 100 kHz. En revanche, si la fréquence centrale est 2,4 GHz, la largeur de la bande peut être de plusieurs dizaines de MHz. Ceci dit, rien n'empêche d'utiliser une bande étroite dans les hautes fréquences.

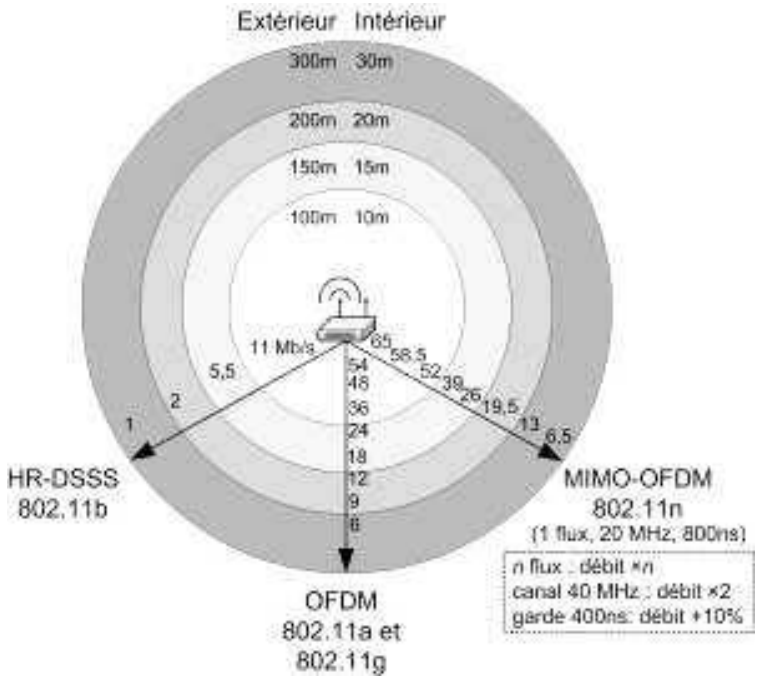


Figure 2.5 — Débit théorique maximal du signal en fonction de la distance.

disponibles pour communiquer dans le 5 GHz que dans le 2,4 GHz, donc la capacité totale du 802.11a est plus importante.

Pour résumer ce qui précède, il existe une formule assez simple, établie par Claude Shannon, mathématicien et père de la fameuse théorie de l'Information. Cette formule permet de trouver le débit maximal en fonction du RSB et de la largeur de la bande de fréquence utilisée :

$$C = H \times \log_2\left(1 + \frac{P_S}{P_B}\right)$$

- C est la capacité maximale du canal de communication, en bits par seconde ;
- H est la largeur de la bande de fréquence utilisée, en hertz ;
- la fonction $\log_2$ est le logarithme binaire : $\log_2(x) = \log(x)/\log(2)$;
- P_S est la puissance du signal, en Watt ;
- P_B est la puissance du bruit, également en Watt.

Par exemple, prenons le cas du WiFi à 2,4 GHz. Les communications ont lieu sur des canaux de fréquences d'une largeur de 22 MHz, donc $H = 22 \times 10^6$ Hz. Admettons que les stations soient relativement proches les unes des autres et qu'il y ait peu de bruit. On peut alors imaginer que le RSB, exprimé en décibels, soit égal à 20 dB. Pour calculer le rapport P_S/P_B, on applique la formule suivante : $P_S/P_B = 10\hat{}(RSB_{dB}/10)$. Dans notre exemple, on obtient $P_S/P_B = 10\hat{}(20/10) = 100$. La capacité maximale théorique du canal de communication est donc égale à :

$$C = 22 \times 10^6 \times \log_2(1 + 100) \approx 146 \times 10^6 \text{ b/s} \approx 140 \text{ Mb/s}$$

Au travers de cet exemple, on constate que le WiFi a de la marge pour progresser et offrir des débits encore plus importants. Cette formule montre par ailleurs qu'en utilisant une bande de fréquence assez large, il est possible de baisser le rapport signal/bruit tout en conservant le même débit. Avec un étalement suffisant, on peut même parvenir à communiquer avec une puissance inférieure à celle du bruit, c'est-à-dire un RSB négatif ! Pour vous en convaincre, reprenez l'exemple précédent avec un RSB négatif, par exemple −2 dB et voyez le résultat. Un récepteur qui se concentrerait sur une seule fréquence ne pourrait alors pas détecter le signal.

> La technique d'étalement de spectre (ou *Spread Spectrum*) permet d'atteindre des débits élevés et de mieux résister au bruit.

La puissance, la fréquence, la largeur de bande, le RSB, la nature et la disposition des obstacles et la qualité des récepteurs décident donc en grande partie de la portée du signal et du débit que l'on peut atteindre. Un autre paramètre important est la modulation radio utilisée. C'est ce que nous allons aborder maintenant.

2.3 LES MODULATIONS RADIO

2.3.1 Les modulations fondamentales

Aucune modulation

Prenons l'exemple d'un opéra retransmis sur une chaîne de radio : comment la musique, c'est-à-dire un signal audio, peut-elle être acheminée par le biais des ondes électromagnétiques ? Les ondes sonores audibles ont des fréquences comprises entre 20 Hz pour les graves et 20 kHz pour les aigus. Il serait tentant de simplement convertir l'onde sonore en onde radio de même fréquence. Malheureusement, il y aurait alors plusieurs problèmes : d'abord, les fréquences radio aussi basses sont très difficiles à produire et à capter ; ensuite, deux émissions de radio simultanées se superposeraient puisqu'elles seraient émises sur la même bande de fréquence (de 20 Hz à 20 kHz) et ce serait la cacophonie.

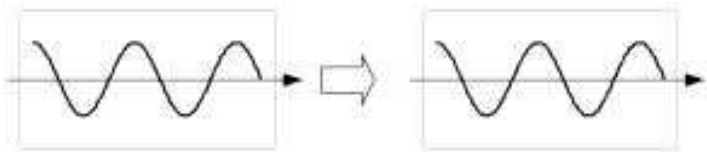


Figure 2.6 — Aucune modulation : le signal source est émis tel quel (irréaliste).

Modulation d'amplitude

Pour résoudre ce problème, une solution consiste à émettre une onde radio de fréquence fixe, que l'on appelle l'onde « porteuse », dont on modifie l'amplitude en fonction de l'onde sonore, qui est l'onde « source » : c'est la modulation d'amplitude (*Amplitude Modulation*, AM). On dit que l'onde source « module » l'onde porteuse, ce n'est possible que si l'onde porteuse a une fréquence bien plus élevée que l'onde source. L'avantage est que l'on peut alors choisir la fréquence que l'on préfère pour le signal porteur, ce qui permet d'émettre plusieurs émissions en même temps sur des fréquences différentes. Le récepteur n'a plus qu'à sélectionner un « canal », c'est-à-dire une fréquence à « démoduler », pour choisir l'émission qu'il préfère. C'est ce que vous faites lorsque vous choisissez une radio AM sur votre chaîne Hi-Fi.

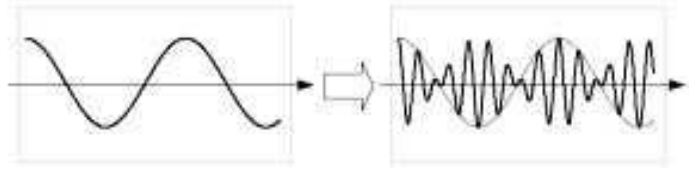


Figure 2.7 — La modulation d'amplitude.

Modulation de fréquence

Inversement, on peut émettre une onde radio d'amplitude fixe, mais dont la fréquence varie au sein d'une bande de fréquences donnée, de façon proportionnelle au signal source. Il s'agit alors de la modulation de fréquence (*Frequency Modulation*, FM).

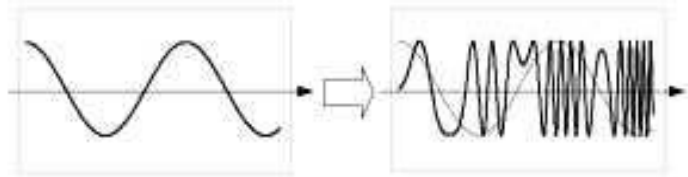


Figure 2.8 — La modulation de fréquence.

Chaque modulation a ses avantages et ses inconvénients :

- L'AM est plus simple à mettre en œuvre techniquement et elle est la première à avoir vu le jour. Elle occupe une bande de fréquences très réduite : théoriquement, une seule fréquence par communication, mais dans la pratique plutôt quelques kHz pour éviter les interférences entre canaux voisins.
- De son côté, la FM a besoin d'une bande assez large : plusieurs dizaines de kHz pour une station de radio, par exemple.
- La FM peut être utilisée à des puissances très faibles alors que l'AM a besoin de plus de puissance car c'est elle qui est modulée par le signal source.

- Symétriquement, l'AM peut se contenter d'une onde porteuse de fréquence assez basse alors que la FM nécessite des fréquences plus élevées.
- La FM est beaucoup moins sensible aux distorsions de puissance dues aux obstacles ou aux interférences puisque les variations de l'intensité du signal ne sont pas prises en compte par le récepteur au cours de la démodulation. Vous vous en rendrez compte si vous écoutez une radio FM lors d'un trajet en voiture en ville : à moins de passer dans un tunnel, le volume du son restera constant. En revanche, si vous écoutez une radio AM, vous entendrez parfois des baisses de volume selon la qualité de la réception.

Tout ceci explique pourquoi l'AM est préférée pour les communications à longue distance (basse fréquence et puissance élevée) et la FM est préférée pour les transmissions en milieu urbain (meilleure résistance aux interférences). Cette comparaison a pour but de vous montrer à quel point le choix de la modulation peut impacter la portée et le débit d'une transmission.

Modulation de phase

La phase d'une onde représente sa position dans le temps : si deux ondes de même fréquence sont en phase, alors leurs pics d'amplitude sont simultanés. Elles sont en opposition de phase lorsque les pics de l'une correspondent aux creux de l'autre. On mesure la phase en degrés : deux ondes *en phase* n'ont aucun décalage, c'est-à-dire une phase égale à 0°. Deux ondes *en opposition de phase* ont un décalage de 180°. Il est possible de moduler la phase en fonction du signal source, ce qu'on appelle simplement la modulation de phase (*Phase Modulation*, PM).

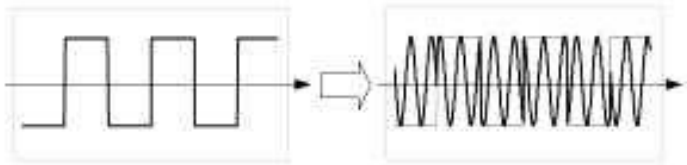


Figure 2.9 — La modulation de phase (plus claire avec un signal source carré).

2.3.2 Les modulations numériques

Modulations simples : ASK, FSK et PSK

Lorsque l'on souhaite transmettre des informations numériques (des 0 et des 1, c'est-à-dire des bits d'information) plutôt qu'une source analogique (comme une onde sonore), on peut utiliser les modulations AM, FM ou PM. On parle alors de « codage » (*keying*).

Pour l'AM, il y aura simplement deux amplitudes possibles, l'une symbolisant le 0 et l'autre le 1. C'est ce qu'on appelle l'*Amplitude-Shift Keying* (ASK), c'est-à-dire le « codage par décalage d'amplitude ». Cette modulation est malheureusement très sensible au bruit et aux interférences.

De même, en FM, on émettra une fréquence donnée pour symboliser le 0 et une autre pour le 1. Cela s'appelle le *Frequency-Shift Keying* (FSK), c'est une technique utilisée par le WiFi comme nous le verrons dans les paragraphes suivants.

En modulation de phase, on pourra choisir une phase de 0° pour coder le 0, ou de 180° pour coder le 1. C'est ce qu'on appelle le *Phase-Shift Keying* (PSK).

Modulations différentielles : DPSK

Une autre technique consiste à prendre en compte la variation de phase et non la phase dans l'absolu : aucun changement de phase signifie « 0 » ; un changement de 180° signifie « 1 ». C'est le *Differential PSK* (DPSK). On pourrait également appliquer la même logique à l'ASK et au FSK.

Malheureusement, les modulations différentielles sont souvent moins performantes en environnement bruyant car elles introduisent une nouvelle source d'erreur possible : le décalage du signal précédent vient se rajouter à celui du signal actuel. Par exemple, en PSK simple, si les signaux émis ont successivement pour phase 0°, 180° et 0° mais que le récepteur reçoit 0°, 120° et 40°, il pourra « arrondir » aux valeurs possibles les plus proches (0° ou 180°) et retrouver le bon résultat. En revanche, avec le même scénario, en DPSK, alors que l'émetteur a transmis deux transitions de 180° chacune, le récepteur verra une transition de 120° (arrondie à 180°) et une de −80° (arrondie à 0°).

L'avantage des modulations différentielles est qu'elles sont plus simples à mettre en œuvre que des systèmes « absolus » : le récepteur peut en effet se calibrer à tout instant sur le dernier signal reçu.

Symboles à bits multiples : QPSK, QAM...

On peut aller plus loin avec le PSK en choisissant quatre phases possibles plutôt que deux (le raisonnement est identique pour les autres modulations). Ces quatre phases auront alors les significations binaires suivantes : 00, 01, 10 et 11. On peut donc transmettre les bits d'information par couples, ce qui double naturellement le débit. Cette technique s'appelle la *Quadrature PSK* (QPSK ou 4PSK).

Les groupes de bits sont appelés des « symboles » ou des « échantillons » (*sample*). On peut donc mesurer le débit en symboles par seconde. Par exemple, un débit de 1 Ms/s (mégasymbole par seconde) avec des symboles de 2 bits correspond bien sûr à un débit de 2 Mb/s. On parle également en bauds, avec 1 baud = 1 symbole/seconde.

> Les bits d'information peuvent être regroupés et émis sous la forme de « symboles ».
> Le débit se calcule alors par la formule suivante :
> Débit = (symboles/seconde) × (bits/symbole)

Le PSK peut être combiné avec la modulation d'amplitude pour coder encore plus de bits d'information dans chaque symbole. Cette technique s'appelle le *Quadrature Amplitude Modulation* (QAM). On pourra par exemple avoir quatre phases possibles (ou transitions de phase avec le DPSK) et deux amplitudes possibles pour chaque

phase. Dans ce cas, on aura huit combinaisons possibles, soit 3 bits d'information pour chaque symbole émis (car $2^3 = 8$) : on parle alors de 8QAM. Comme nous le verrons, pour les débits les plus élevés, le WiFi repose sur le 16QAM (douze phases possibles dont quatre pour lesquelles deux amplitudes sont possibles) avec 4 bits d'information par symbole, ou même le 64QAM avec 6 bits par symbole ! Le QAM requiert toutefois un matériel assez sophistiqué.

Filtre gaussien : GFSK

Une autre technique de modulation assez complexe consiste à faire passer la source binaire au travers d'un filtre gaussien avant de moduler la porteuse. Avant le passage dans le filtre la source possède deux états (0 et 1) et les transitions entre ces états sont brutales : en d'autres termes, le signal est « carré ». Une fois passé au travers du filtre, le signal source est « adouci », les transitions sont moins brutales. Cela revient en quelque sorte à étaler chaque bit et à le faire déborder sur son voisin.

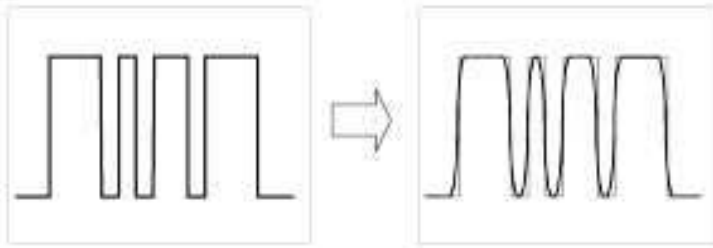


Figure 2.10 — Un signal carré passant au travers d'un filtre Gaussien.

Ensuite, n'importe quelle modulation peut être appliquée à cette source adoucie, comme le FSK, par exemple : on parle alors de FSK Gaussien, noté GFSK.

Sans le filtre Gaussien, les transitions d'état brutales provoquent l'apparition de fréquences harmoniques dans le signal émis[1]. Ceci a pour conséquence d'étaler le spectre occupé par le signal et donc de provoquer des interférences avec les canaux voisins. Grâce au GFSK, les transitions d'état sont adoucies, ce qui limite considérablement le débordement du signal hors de la bande de fréquence choisie, comme on le voit sur la figure 2.11.

Il existe une relation directe entre le nombre de bits par secondes de la source (c'est-à-dire son débit) et la largeur de la bande principale occupée par le signal : plus le débit est important, plus les transitions d'état sont fréquentes, donc plus les harmoniques sont nombreuses et plus le spectre du signal est étalé. Avec le FSK et le PSK ou encore le QAM, la largeur de la bande principale est environ égale au double du débit : par exemple, pour un débit de 11 Mb/s, la bande principale occupe 22 MHz. Cet étalement du spectre peut être intéressant, car comme nous l'avons vu, il permet de mieux résister au bruit. Nous verrons que la modulation DSSS repose

1. L'explication physique serait un peu longue à présenter mais l'idée est qu'un signal carré est composé de multiples ondes : ce sont les harmoniques.

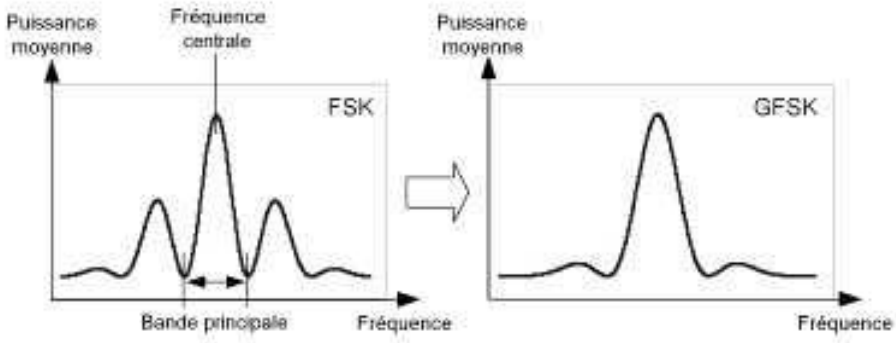


Figure 2.11 — Atténuation des fréquences harmoniques grâce au filtre Gaussien.

sur ce principe. Selon le contexte, il peut être utile de « condenser » le signal sur un canal étroit, ou bien au contraire de l'étaler sur un spectre large.

> La bande de fréquence principale occupée par un signal binaire modulé en FSK, PSK ou QAM est environ égale au double du débit de la source. Par exemple, pour un débit de 11 Mb/s, la bande principale a une largeur de 22 MHz.

Les modulations d'impulsions

Un dernier type de modulation numérique consiste à émettre des impulsions régulières et à les décaler dans le temps en fonction du signal source. Le temps est découpé en tranches d'une durée fixe et pendant chaque tranche de temps une brève impulsion est émise, d'une durée bien inférieure à celle de la tranche. Le signal source module la position de l'impulsion dans la tranche. Par exemple, on peut convenir que si l'impulsion a lieu au début de la tranche, cela correspond au bit 0 et si elle se situe à la fin, il s'agit du bit 1.

Plutôt que de modifier la position de l'impulsion dans le temps, il est également possible de modifier sa durée, son amplitude, etc. Une combinaison de ces modulations est également possible.

La couche physique infrarouge définie par le 802.11 repose sur la modulation de position d'impulsions, mais sachant que la couche infrarouge n'est pas utilisée, nous ne détaillerons pas davantage cette modulation.

Comparaison des modulations

Les différentes modulations que nous venons de voir n'ont pas toutes les mêmes caractéristiques :

- le PSK et ses variantes permettent d'atteindre des débits très élevés, mais ils « débordent » sur les canaux voisins, donc les interférences inter-canaux (*Inter-Carrier Interference*, ICI) sont à craindre ;

- le 2PSK offre un débit moins élevé que le 4PSK, lui-même moins rapide que le 8PSK et ainsi de suite ;
- en revanche, le 2PSK est moins sensible au bruit que le 4PSK, lui-même moins sensible que le 8PSK, etc. ;
- le 64QAM est 1,5 fois plus rapide que le 16PSK et est aussi résistant au bruit, mais il suppose un matériel plus complexe ;
- le DPSK est légèrement moins performant que le PSK mais plus simple à mettre en œuvre ;
- le GFSK est moins rapide que le PSK, mais il est moins sensible au bruit ;
- le GFSK déborde très peu de la bande de fréquence qu'il utilise, ce qui le rend très efficace lorsque plusieurs canaux voisins sont utilisés simultanément.

Il est temps maintenant d'aborder les modulations du WiFi, qui reposent sur les modulations que nous venons de voir. Elles sont au nombre de trois :

- *Frequency Hopping Spread Spectrum* (FHSS) ;
- *Direct Sequence Spread Spectrum* (DSSS) ;
- *Orthogonal Frequency Division Multiplexing* (OFDM).

Le FHSS n'est utilisé que dans la première version du standard 802.11. Le 802.11a repose exclusivement sur l'OFDM, le 802.11b exclusivement sur le DSSS et le 802.11g utilise le DSSS ou l'OFDM, en fonction du débit souhaité. Le 802.11n repose sur l'OFDM exclusivement lorsqu'on le règle sur un canal à 5 GHz, et sur le DSSS ou l'OFDM à 2,4 GHz.

2.3.3 Le FHSS

La modulation FHSS (*Frequency Hopping Spread Spectrum*) a été inventée et brevetée en 1942 par l'actrice Hedy Lamarr et le pianiste George Antheil, qui étaient assez polyvalents ! Le principe du FHSS est assez simple : une large bande de fréquences est divisée en de multiples canaux et les communications se font en sautant (*hopping*) successivement d'un canal à un autre, selon une séquence et un rythme convenus à l'avance entre l'émetteur et le récepteur.

Il est difficile d'intercepter les communications si l'on ne connaît pas la séquence choisie, c'est pourquoi elle fut très appréciée par les militaires américains qui l'utilisèrent pour radioguider les torpilles sans que l'ennemi puisse intercepter ou brouiller le signal. Dans le cas du 802.11, cette fonction n'est (malheureusement) pas exploitée car les séquences de canaux utilisées ne sont pas secrètes.

Le FHSS offre également une résistance importante aux interférences voire même aux brouillages volontaires car les canaux pour lesquels le bruit est trop important peuvent être simplement évités. Toutefois, le 802.11 FHSS n'exploite pas cette capacité, contrairement au Bluetooth et au HomeRF qui sont deux technologies sans fil utilisant la modulation FHSS.

Un dernier avantage du FHSS est que plusieurs communications peuvent avoir lieu en même temps sur la même bande de fréquences pourvu qu'elles utilisent des

séquences de canaux ne rentrant pas en collision les unes avec les autres. Par exemple, une communication pourrait utiliser la séquence triviale : 1,2,3,1,2,3,1,2,3... tandis qu'une autre communication aurait la séquence suivante : 2,3,1,2,3,1,2,3,1... de sorte qu'à aucun moment les deux communications n'utilisent le même canal.

En contrepartie, chaque communication a un débit relativement faible puisqu'elle n'exploite qu'un seul canal assez étroit à la fois.

Dans la première version du 802.11, la bande de fréquences allant de 2 400 MHz à 2 483,5 MHz a été découpée pour le FHSS en canaux de 1 MHz de largeur chacun. Dans la plupart des pays, les canaux 2 à 80 sont autorisés (de 2 401 MHz à 2 480 MHz). Au sein de chaque canal, la modulation gaussienne FSK à deux états (2GFSK) est utilisée et permet un débit de 1 Mb/s. En utilisant la modulation 4GFSK (GFSK à quatre états, soit 2 bits par symbole) on peut atteindre 2 Mb/s. En utilisant le GFSK comme modulation sous-jacente, le FHSS permet d'éviter les interférences entre canaux voisins, ce qui permet à plusieurs utilisateurs de communiquer en FHSS en même temps sans se gêner.

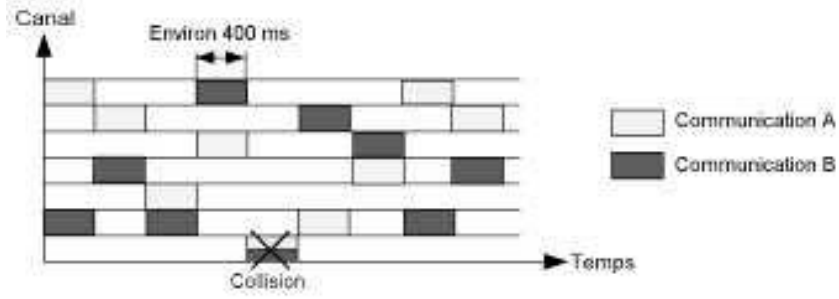


Figure 2.12 — Exemple de partage des ondes avec le FHSS.

Le standard 802.11 a défini un mécanisme d'adaptation dynamique du débit en fonction du rapport signal/bruit : lorsqu'il est élevé, la modulation utilisée est la 4GFSK à 2 Mb/s, sinon le 802.11 s'adapte automatiquement et « descend » au 2GFSK à 1 Mb/s.

2.3.4 Le DSSS

Le chipping

La modulation DSSS (*Direct Sequence Spread Spectrum*) est également une technique d'étalement de spectre, mais contrairement au FHSS, aucun saut de fréquence n'a lieu : le DSSS provoque des transitions d'état très rapides (*chipping*) qui tendent à étaler le spectre du signal : en effet, nous avons vu au § 2.3.2 qu'avec les modulations FSK, PSK et QAM la largeur du spectre correspondait au double du débit de la source. En provoquant « artificiellement » un débit très élevé, le spectre est étalé.

Pour ce faire, l'émetteur envoie une séquence de plusieurs bits, appelés des *chips*, pour chaque bit d'information à transmettre. Par exemple, on peut choisir d'envoyer

11101 au lieu de 0 et son inverse (00010) au lieu de 1 : dans ce cas, si l'on veut transmettre l'information 010, alors on émettra les *chips* suivants : 11101 00010 11101. Dans cet exemple, la séquence 11101 est ce qu'on appelle le « code d'étalement ». Plus ce code est long, plus le débit est artificiellement démultiplié, donc plus le spectre est étalé. Par exemple, si le débit des données à envoyer est égal à 1 Mb/s, mais qu'on utilise un code d'étalement de 11 chips, alors le débit de chips sera bien sûr égal à 11 Mb/s : du coup, la bande de fréquence occupée par le signal aura une largeur égale à 22 MHz car la largeur de la bande occupée par le signal est égale au double du débit de la source. Sans ce *chipping*, la bande occupée n'aurait qu'une largeur de 2 MHz (deux fois 1 Mb/s).

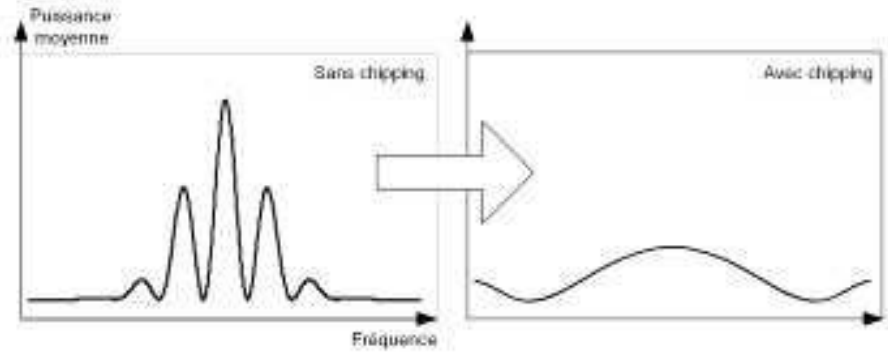


Figure 2.13 — Étalement de spectre grâce à la technique du *chipping*.

Le DSSS présente deux intérêts importants :

- tout d'abord, comme nous l'avons dit, le spectre de fréquences du signal est étalé, avec tous les avantages (et les inconvénients) que cela apporte, en particulier une meilleure résistance au bruit ;
- le fait que l'on émette plusieurs chips pour chaque bit d'information signifie que l'on peut avoir une redondance importante, qui permet de corriger des erreurs de transmission. Par exemple, dans l'exemple précédent, puisque le récepteur connaît le code d'étalement utilisé (11101), alors il sait qu'il ne devrait recevoir que 11101 (pour le bit d'information 0) ou 00010 (pour le bit 1). S'il reçoit 00110, il pourra facilement corriger l'erreur en estimant que le plus proche est 00010 (correspondant au bit 1).

La modulation DSSS étale le spectre du signal par une technique de *chipping*. Ceci permet avant tout de mieux résister au bruit.

Le 802.11 a défini quatorze canaux de 22 MHz de large, dans la même bande de fréquences à 2,4 GHz que le FHSS. Pour communiquer, l'émetteur et le récepteur doivent se mettre d'accord sur un canal fixe à utiliser. Pour un débit de 1 Mb/s, le 802.11 DSSS repose sur la modulation 2DPSK que nous avons vue au § 2.3.2. Pour le débit de 2 Mb/s, le DSSS utilise simplement la modulation 4DPSK.

Dans les deux cas, le code d'étalement a une longueur de 11 bits et il est toujours égal à 10110111000. Ce code fait partie d'une famille de codes aux propriétés mathématiques similaires, définie en 1953 par le mathématicien Barker : ils favorisent un bon étalement de spectre (comme ne le ferait pas, par exemple, le code 11111111111) et leur format les rend bien adaptés pour synchroniser l'émetteur et le récepteur, ce qui permet de limiter les problèmes dus au *multipath*.

La modulation CCK

Pour atteindre des débits de 5,5 Mb/s ou 11 Mb/s, le 802.11b a amélioré encore ce procédé en utilisant la modulation *Complementary Code Keying* (CCK) pour atteindre ce qu'on appelle le DSSS à haute vitesse ou *High-Rate DSSS* (HR-DSSS). Celle-ci repose toujours sur le même principe de base d'étalement par *chipping* avec la modulation 4DPSK. Toutefois, au lieu d'utiliser toujours le même code de Barker pour étaler le signal, elle utilise jusqu'à 64 codes différents, ce qui permet de transporter 6 bits d'information (car $2^6 = 64$) en plus des deux bits autorisés par la modulation 4DPSK. Ces codes, de 8 bits de longueur chacun, sont des « codes complémentaires » c'est-à-dire que leurs propriétés mathématiques permettent aux récepteurs de ne pas les confondre, même s'il y a quelques erreurs de transmission, voire même un décalage dans la réception dû au multipath. Puisqu'il y a nettement moins de redondance, on obtient un débit plus important, en tout cas tant que la réception est bonne (donc à faible distance). Puisque la résistance au multipath est meilleure, le HR-DSSS est mieux adapté en intérieur et à courtes distances que le DSSS sur Barker.

Malheureusement, alors que le FHSS peut sauter les canaux encombrés par du bruit ou des interférences, le DSSS ne le peut pas : s'il y a d'autres réseaux sans fil à proximité exploitant le même canal, le DSSS en souffrira considérablement. Sachant que la technologie Bluetooth repose sur le FHSS, sur les mêmes fréquences à 2,4 GHz, on comprend pourquoi le 802.11 DSSS souffre de la présence d'équipements Bluetooth à proximité. En revanche, le Bluetooth supporte à peu près la présence d'équipements 802.11 DSSS. Pour résumer, le DSSS supporte mieux le bruit homogène (bruit « blanc ») que le FHSS et inversement, le FHSS supporte mieux le bruit focalisé sur une fréquence particulière que le DSSS.

Comme pour le FHSS, le standard définit pour le DSSS un mécanisme d'adaptation automatique du débit en fonction de la distance. Ainsi, à courte distance la modulation sera le HR-DSSS à 11 Mb/s (8 bits d'information pour 8 *chips* émis). Plus, loin, on passe automatiquement à 5,5 Mb/s (4 bits d'information pour 8 *chips* émis). Ensuite, on descend à 2 Mb/s en utilisant le DSSS/Barker et 4DPSK, puis à 1 Mb/s en DSSS/Barker et 2DPSK.

2.3.5 L'OFDM

La modulation OFDM (*Orthogonal Frequency Division Multiplexing*), parfois appelée *Discrete Multitone Modulation* (DMT), est sans doute la plus puissante des trois modulations du WiFi car elle permet à la fois les débits les plus importants, la meilleure résistance au *multipath*, mais aussi la plus grande capacité de partage du spectre : elle est

donc particulièrement indiquée en intérieur avec une densité importante d'antennes WiFi. On la trouve à la fois dans le 802.11g, le 802.11a et dans le 802.11n. D'autres technologies l'exploitent, dont en particulier la technologie *Digital Subscriber Line* (DSL) ou encore le Wimax.

L'OFDM repose sur le principe du multiplexage : permettre la transmission simultanée de plusieurs communications sur une même bande de fréquences. Il existe le multiplexage par division des communications au cours du temps, qu'on appelle le *Time Division Multiplexing* (TDM) : chaque communication dispose de sa tranche de temps pour émettre des données et peut utiliser l'ensemble du spectre. Le multiplexage peut également se faire en partageant les différentes communications par fréquences : c'est le *Frequency Division Multiplexing* (FDM). Un spectre assez large est divisé en de multiples sous-porteuses (*sub-carriers*) et les données sont émises simultanément sur chaque sous-porteuse. Malheureusement, il est alors possible d'avoir des interférences entre les sous-porteuses, ce qu'on appelle l'*Inter-Carrier Interference* (ICI). Pour résoudre ce problème, l'OFDM utilise une fonction mathématique assez complexe pour rendre les sous-porteuses « orthogonales », c'est-à-dire pour qu'elles n'interfèrent pas les unes avec les autres. Dans le cas du 802.11, il s'agit d'une transformation de Fourier inverse rapide (*Inverse Fast Fourier Transform*, IFFT). Grâce à cette fonction, les porteuses sont placées dans le spectre de fréquences de telle sorte que les pics de puissance d'une porteuse donnée correspondent aux zéros des autres porteuses.

En WiFi, 52 sous-porteuses d'environ 312,5 kHz chacune permettent de couvrir un spectre de 16,66 MHz, qui forme un canal de communication OFDM. Chaque sous-porteuse est modulée en PSK (2PSK ou 4PSK) ou en QAM (16QAM ou 64QAM). Sur ces 52 sous-porteuses, le WiFi en utilise quatre comme « pilotes » qui servent à synchroniser les fréquences et à mesurer en permanence les interférences et les décalages de phase, afin de s'y adapter au mieux. Ainsi, les données à émettre sont groupées en symboles de 48 bits en 2PSK (et six fois plus en 64QAM par exemple). Ces symboles sont émis en 48 portions simultanées : une par sous-porteuse.

Puisqu'on émet de nombreux bits simultanément, on peut se permettre de diminuer le nombre de symboles émis par seconde tout en conservant un bon débit en termes de bits par seconde. Ceci permet de limiter considérablement le risque de perturbations dues au multipath, car il est alors peu probable qu'un symbole arrivera en même temps que le symbole suivant (car il y a un laps de temps important entre les deux).

Enfin, l'OFDM peut être renforcé par des codes « convolutifs » (on parle de *Coded OFDM* ou COFDM) : il s'agit d'un codage qui rajoute de la redondance dans le message à transmettre et permet ainsi au récepteur de corriger les erreurs de transmission. À la réception, un algorithme sophistiqué est utilisé pour retrouver le message original le plus probable (par exemple l'algorithme de Viterbi). En rajoutant une redondance plus ou moins importante, ce mécanisme permet une bonne résistance aux interférences. Plus on souhaite un débit élevé, moins la redondance doit être importante : en conséquence, les débits élevés sont plus sensibles aux interférences. De plus, l'étalement du spectre étant assez homogène (contrairement au DSSS), un signal OFDM ne provoque que peu d'interférences pour les autres équipements sans fil présents.

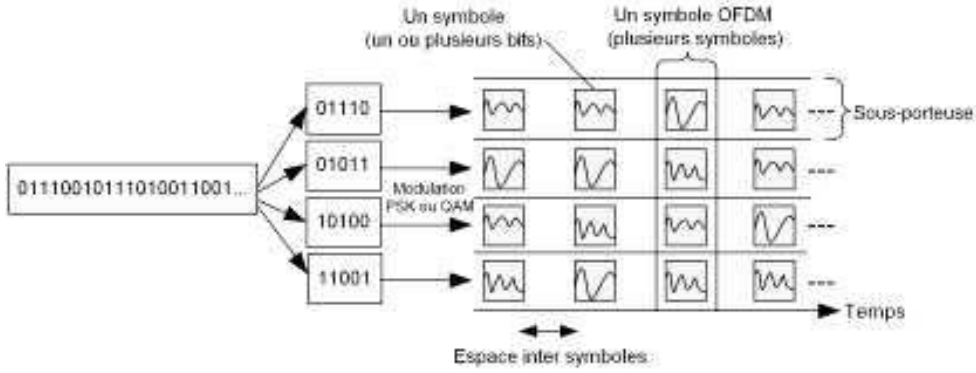


Figure 2.14 — La modulation OFDM.

La modulation OFDM utilise simultanément de multiples sous-porteuses et permet d'atteindre des débits très élevés. Chaque symbole transporte de nombreux bits d'information : il est possible d'espacer les symboles tout en conservant un bon débit. Cela permet de limiter les effets du multipath.

Le 802.11 définit comment modifier, en fonction de l'environnement radio, la modulation des sous-porteuses, le nombre de symboles par seconde et le niveau de redondance des codes convolutifs. En fonction de la qualité du signal, le débit passera alors automatiquement de 54 Mb/s à 48 Mb/s, puis 36 Mb/s, puis 24 Mb/s, puis 18 Mb/s, puis 12 Mb/s, puis 9 Mb/s et enfin 6 Mb/s. Le 802.11g pourra même passer à la modulation HR-DSSS (11 Mb/s et 5,5 Mb/s) ou DSSS (2 Mb/s et 1 Mb/s).

2.3.6 Techniques multi-antennes

La plupart des points d'accès et même de nombreux adaptateurs WiFi sont équipés de plusieurs antennes. Celles-ci sont mises à profit en WiFi pour améliorer la portée, la fiabilité ou encore le débit des communications, à l'aide de plusieurs techniques assez sophistiquées. Nous allons présenter les plus importantes d'entre elles.

SISO, SIMO, MISO, MIMO

Précisons tout d'abord le vocabulaire :

- Si l'émetteur n'utilise qu'une seule antenne pour émettre et le récepteur n'utilise qu'une seule antenne pour recevoir, on parle de *Single Input Single Output* (SISO).
- Si l'émetteur n'utilise toujours qu'une seule antenne mais que le récepteur en utilise plusieurs, alors on parle de *Single Input Multiple Output* (SIMO).
- Si l'émetteur utilise plusieurs antennes et le récepteur une seule, on parle de *Multiple Input Single Output* (MISO).

- S'il y a plusieurs antennes en émission et en réception, il s'agit de *Multiple Input Single Output* (MIMO). Les mots *input* et *output* (entrée et sortie) sont ici utilisés dans un sens qui peut surprendre : l'entrée correspond à l'émission (c'est l'entrée dans « l'interface air »), et la sortie correspond à la réception (la sortie de « l'interface air »).

La figure 2.15 présente ces quatre configurations possibles, en représentant les différents chemins que le signal peut emprunter en présence d'un obstacle.

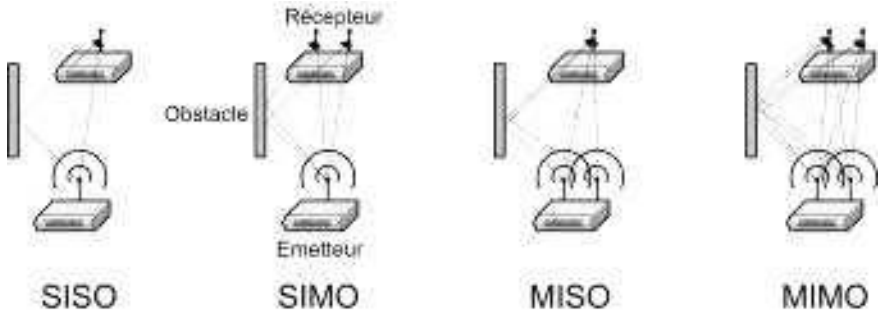


Figure 2.15 — Les quatre configurations SISO, SIMO, MISO et MIMO.

Notons au passage que le MIMO ne désigne pas une technique unique, mais plutôt toutes les techniques reposant sur des antennes multiples à la fois du côté de l'émetteur et du récepteur, sur un unique canal radio. La norme 802.11n exploite plusieurs techniques MIMO et MISO pour améliorer considérablement le débit, la portée et la fiabilité du WiFi. Avant d'aborder ces techniques, commençons par deux techniques multi-antennes bien plus anciennes que le 802.11n : la diversité d'espace et le *beamforming*.

Diversité d'espace

Depuis plusieurs années déjà la plupart des points d'accès ont deux antennes : une seule sert à l'émission, mais les deux servent à la réception[1]. À quoi servent donc ces deux antennes ? Elles permettent de faire ce qu'on appelle de la « diversité d'espace » à la réception. La mise en œuvre la plus simple de ce principe consiste simplement à écouter sur les deux antennes à la fois, et à sélectionner à tout moment le signal de l'antenne qui reçoit le mieux. Ceci est surtout utile pour résister aux interférences dues aux multiples chemins qu'empruntent les ondes pour arriver à leur destination (ce qu'on appelle le « *multipath* »).

Précisons ce point : si une partie du signal émis suit un chemin indirect avant d'arriver au récepteur, en se reflétant contre un obstacle par exemple (comme dans la figure 2.15), alors il arrivera avec un léger retard, et risquera alors d'être en opposition

1. Si une station connectée à un tel point d'accès n'a qu'une seule antenne, alors on est en configuration SISO de l'AP vers la station, et en configuration SIMO de la station vers l'AP.

de phase avec le signal qui aura suivi le chemin le plus court, ce qui diminuera la puissance du signal reçu[1]. Mais si l'on a plusieurs antennes à la réception, et qu'elles sont espacées judicieusement, alors la probabilité qu'il y ait opposition de phase sur les deux antennes à la fois sera faible (voir le chapitre 5, figure 5.10). En choisissant toujours l'antenne qui a le plus fort signal, on résiste donc mieux à ce type d'interférences. Notons que les algorithmes sont parfois plus sophistiqués et combinent le signal reçu sur les deux antennes, plutôt que de retenir uniquement le plus fort.

Cette technique permet donc de mieux résister aux interférences dues à la présence d'obstacles (notamment en intérieur). Elle a l'avantage d'être entièrement mise en œuvre du côté du récepteur, sans la moindre participation de l'émetteur. Elle ne fait pas partie du standard 802.11, néanmoins le fait qu'elle puisse être mise en œuvre sans contrainte pour le reste du réseau explique pourquoi la plupart des points d'accès l'utilisent.

Beamforming

On voit sur le marché, depuis plusieurs années, des antennes « intelligentes » qui exploitent une technique appelée le « *beamforming* », littéralement la « formation de faisceaux ». Une antenne intelligente est en réalité composée de multiples antennes classiques qu'elle synchronise de façon à former une sorte de faisceau de rayonnement en direction de chaque utilisateur. La figure 2.16 illustre le principe de cette technique. Un point d'accès est ici muni de deux antennes (ou d'une seule antenne « intelligente » composée de deux antennes) et il doit envoyer un message à un utilisateur.

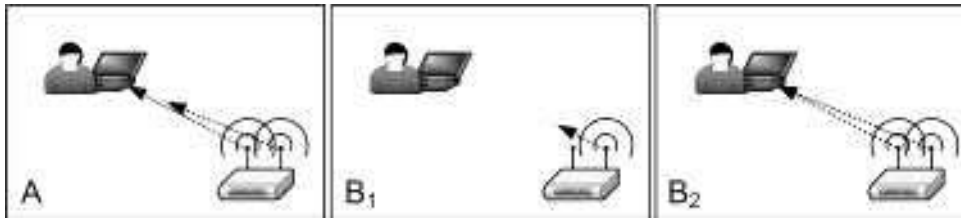


Figure 2.16 — Principe de fonctionnement du *beamforming*.

Admettons (A) que le point d'accès émette le message simultanément sur ses deux antennes. Puisque l'utilisateur se situe sur la gauche, il recevra les ondes émises par l'antenne de gauche très légèrement avant les ondes émises par l'antenne de droite. Ces ondes risquent donc d'être en décalage de phase : si c'est le cas le récepteur risquera malheureusement de recevoir un signal affaibli (parfois même plus faible encore que si l'AP n'avait utilisé qu'une seule antenne pour émettre le message). La

1. De façon analogue, lorsqu'une vague rencontre le bord d'une piscine et qu'elle rebondit, elle croise les vagues qui n'ont pas rebondi. Lorsque deux sommets de vagues se rencontrent, cela donne une vague dont l'amplitude (la hauteur) est la somme de l'amplitude des deux vagues : l'interférence est constructive. Inversement, si le sommet d'une vague rencontre le creux d'une autre vague, les deux peuvent s'annuler : l'interférence est destructive.

technique du *beamforming* consiste à décaler dans le temps l'émission du signal sur les différentes antennes. Dans notre exemple, le point d'accès commence par émettre le signal uniquement sur l'antenne de droite (B_1), et après un très bref instant il commence à émettre également sur l'antenne de gauche (B_2). De cette façon, les deux ondes parviendront exactement en même temps à destination : elles seront donc en phase, et l'amplitude du signal reçu sera égale à la somme de l'amplitude des deux ondes. Le *beamforming* parvient ainsi à amplifier le signal en direction de la station, sans que l'on ait à orienter physiquement les antennes vers le récepteur.

La question qui se pose maintenant est de savoir comment le point d'accès peut bien deviner dans quelle direction se trouve une station afin d'orienter le faisceau vers elle ? La réponse est la suivante : lorsqu'une station envoie un paquet au point d'accès, ce paquet est reçu par les deux antennes du point d'accès avec un léger décalage dans le temps. Il suffit alors de renvoyer la réponse avec le même décalage, mais inversé, pour que le faisceau se forme dans la bonne direction.

Le *beamforming* offre un gain de puissance important, ce qui permet d'atteindre une portée plus importante ou un meilleur rapport signal/bruit permettant d'utiliser une modulation radio plus élevée, donc d'atteindre un débit plus important. En outre, le faisceau reste concentré en direction des récepteurs, pour chaque paquet émis, ce qui permet de limiter les interférences avec les réseaux voisins. Autre avantage du *beamforming* : il est mis en œuvre entièrement au niveau de l'émetteur, de façon entièrement transparente pour les récepteurs (autrement dit, ils n'ont pas besoin de savoir gérer le *beamforming* : ils reçoivent un signal, certes amplifié mais tout à fait normal).

Mais cette technique n'a pas que des atouts : le gain de puissance peut être assez important dans l'axe des faisceaux, et il faut donc faire attention à ne pas dépasser les limites légales de puissance rayonnée. En outre, si le récepteur est en mouvement alors le *beamforming* est moins efficace, voire même nuisible. En effet, comme nous l'avons vu, le faisceau est orienté automatiquement vers l'endroit où se trouvait le récepteur la dernière fois qu'il a envoyé un message. Du coup, s'il s'est déplacé depuis, le faisceau sera mal orienté, donc le gain de puissance sera moins important, voire même négatif : le signal sera alors plus faible que si l'on n'utilisait pas de *beamforming*. Cette technique n'est donc pas adaptée aux usages mobiles[1].

Pour l'instant, cette technique ne fait pas partie du standard 802.11, mais elle peut être mise en œuvre de façon transparente pour le reste du réseau (comme la technique de diversité d'espace).

Multiplexage spatial

La technique MIMO la plus utilisée, notamment dans les produits respectant la norme 802.11n (voir § 2.6) est le multiplexage spatial : les données à émettre sont découpées en plusieurs flux, et chaque flux est émis par une antenne distincte. Lorsque ces flux parviennent aux antennes du récepteur, pourvu qu'ils aient des « signatures

1. Bien souvent les produits qui mettent en œuvre le *beamforming* savent détecter lorsque les récepteurs se déplacent, et ils n'utilisent cette technique que pour les récepteurs immobiles.

spatiales » suffisamment distinctes (c'est-à-dire pourvu qu'ils aient suivi des chemins assez différents), alors le récepteur est capable de les distinguer, de les recevoir correctement et donc de reconstruire les données d'origine. Le multiplexage spatial est donc plus efficace en situation où le *multipath* est important, c'est-à-dire lorsqu'il y a de multiples obstacles et reflets, notamment à l'intérieur des bâtiments. Il n'est pas très efficace lorsque l'émetteur et le récepteur sont en ligne de vue directe.

Pour vous donner une idée de ce principe, imaginez que deux jumeaux vous parlent en même temps, l'un vous racontant la première moitié d'une histoire, et l'autre vous racontant l'autre moitié. Avec un peu d'effort, vous parviendrez peut-être à écouter les deux moitiés de l'histoire, et vous pourrez ainsi reconstituer l'histoire complète. Cela aura pris la moitié du temps qu'il aurait fallu si une seule personne vous avait raconté l'histoire de bout en bout : le débit est donc doublé. La difficulté est bien sûr de parvenir à distinguer les deux voix.

Le principe mathématique du multiplexage spatial est le suivant. Nous prendrons pour exemple le cas où l'émetteur et le récepteur ont chacun deux antennes. La figure 2.17 montre la situation réelle et sa modélisation dans le cadre du multiplexage spatial.

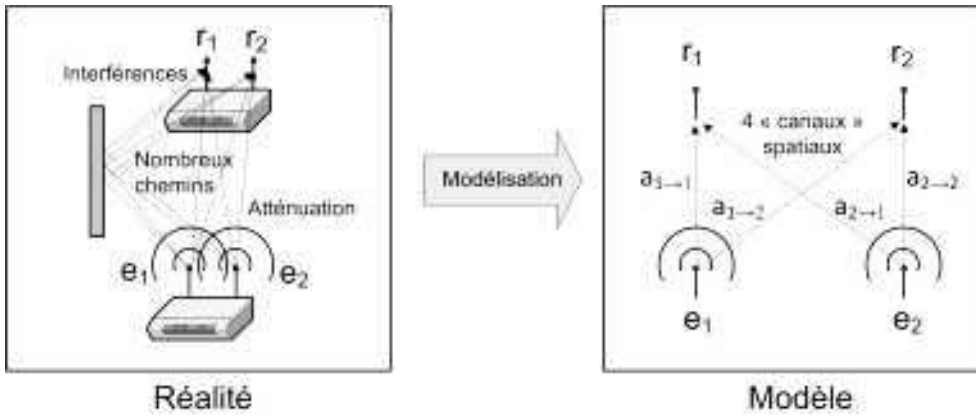


Figure 2.17 — Modèle du multiplexage spatial.

Le signal émis par l'antenne 1 de l'émetteur est noté e_1. Il est capté par l'antenne 1 du récepteur après avoir subi une atténuation notée $a_{1\to1}$. De même, le signal e_2 émis par l'antenne 2 de l'émetteur est capté par l'antenne 1 du récepteur après avoir subi une atténuation notée $a_{2\to1}$. Si l'on suppose que la seule altération d'un signal pendant son trajet est une simple atténuation, due à la distance parcourue et à des interférences (en situation de multipath), alors le signal capté par l'antenne 1 du récepteur, noté r_1, est défini par la formule suivante :

$$r_1 = e_1 \times a_{1\to1} + e_2 \times a_{2\to1}$$

De même, le signal capté par l'antenne 2 du récepteur se calcule ainsi :

$$r_2 = e_1 \times a_{1\to2} + e_2 \times a_{2\to2}$$

Le récepteur ayant reçu r_1 et r_2, s'il peut également estimer la valeur des différentes atténuations ($a_{1\to1}$, $a_{1\to2}$, $a_{2\to1}$, et $a_{2\to2}$) alors il peut retrouver r_1 et r_2 : il s'agit d'une résolution d'un système à deux équations et deux inconnues. Cela vous rappelle-t-il vos cours de mathématiques ? Malheureusement la résolution ne sera possible qu'à condition que les facteurs d'atténuation ne soient pas trop corrélés. Par exemple, si toutes les atténuations sont égales ($a_{1\to1} = a_{1\to2} = a_{2\to1} = a_{2\to2}$) alors le système d'équations n'a pas de solution car les deux équations n'en sont en fait plus qu'une seule, avec toujours deux inconnues (l'atténuation unique est notée a) :

$$r_1 = r_2 = a \times (e_1 + e_2)$$

Ceci n'est pas rare : il suffit par exemple que l'émetteur et le récepteur soient en vision directe, à plusieurs mètres l'un de l'autre, sans le moindre obstacle à proximité. Puisqu'il n'y a pas d'obstacles, seuls les chemins en ligne droite entre les différentes antennes seront empruntés, donc pas d'interférences dues aux chemins multiples : l'atténuation ne dépend alors que de la distance. Puisque l'émetteur et le récepteur sont à plusieurs mètres l'un de l'autre, les quatre chemins entre les antennes de l'émetteur et du récepteur (1→1, 1→2, 2→1 et 2→2) ont tous à peu près la même longueur, donc les atténuations sont presque égales. Le système d'équations ne peut pas être résolu.

Pour que le récepteur puisse résoudre son système d'équations, il faut donc que les paramètres d'atténuation soient aussi peu corrélés que possible : absence de ligne de vue, beaucoup d'obstacles pour refléter les signaux, antennes espacées, émetteur et récepteur proches... Paradoxalement, le débit sera meilleur avec le MIMO si l'on n'est pas en ligne de vue !

Mais ce n'est pas tout : comme nous l'avons vu, le récepteur doit également évaluer la valeur des facteurs d'atténuations pour pouvoir résoudre ses équations. Ceci se fait en permanence, par l'échange régulier d'informations de calibrage entre l'émetteur et le récepteur. Cet échange permet également d'évaluer le niveau de bruit reçu sur chaque antenne du récepteur. Nous avons en effet négligé ce paramètre jusqu'ici pour ne pas alourdir l'explication, mais pour plus de réalisme il faudrait rajouter à droite de la première équation le bruit capté par l'antenne 1 (... + b_1), et à droite de la seconde équation le bruit capté par l'antenne 2 (... + b_2). Pour résoudre ce système d'équations, il est donc nécessaire d'évaluer également le bruit.

La technique de multiplexage spatial est en fait un peu plus complexe, car l'émetteur optimise les signaux qu'il émet sur ses différentes antennes afin de les décorréler au maximum du point de vue du récepteur. Pour cela, il exploite sa connaissance des paramètres d'atténuation et de bruit et emploie des algorithmes assez complexes : la puissance de calcul de l'émetteur doit être importante, ce qui explique en partie pourquoi les équipements WiFi MIMO (et notamment 802.11n) consomment davantage d'énergie et coûtent plus cher que les équipements classiques.

Le nombre de flux émis simultanément est limité par le nombre minimum d'antennes du récepteur ou de l'émetteur. En effet, l'émetteur ne peut évidemment pas émettre plus de flux simultanés qu'il n'a d'antennes, et le récepteur ne peut pas non plus décoder plus de flux qu'il n'a d'antennes, car son système d'équations aurait moins d'équations que d'inconnues, ce qui est impossible à résoudre (on ne peut

pas, par exemple résoudre un système à deux équations et trois inconnues). Donc si l'émetteur a trois antennes et le récepteur en a deux, par exemple, alors (avec le 802.11n) l'émetteur se limitera automatiquement à deux flux simultanés. On parle dans ce cas de MIMO 3 × 2 × 2 : trois antennes à l'émission, deux antennes à la réception et deux flux simultanés. Le 802.11n prévoit au maximum 4 × 4 × 4, ce qui suppose que l'émetteur et le récepteur aient quatre antennes et soient compatibles avec ce mode, mais dans la pratique les produits se limitent, au mieux, à 3 × 3 × 3.

Codage espace-temps

Autre technique permettant d'exploiter de multiples antennes du côté de l'émetteur : le « codage espace-temps » (non ce n'est pas de la science-fiction). En anglais, on parle de « *Space Time Coding* » (STC). Cette technique consiste à émettre la même information plusieurs fois dans l'espace et dans le temps afin que cette redondance améliore la fiabilité de la transmission (on augmente donc le débit réel et la portée). La même information est envoyée *via* plusieurs antennes (redondance dans l'espace) et à plusieurs reprises (redondance dans le temps), mais elle est à chaque fois codée d'une façon différente, selon des algorithmes qui permettent d'optimiser la probabilité de pouvoir correctement reconstruire l'information à l'arrivée.

Il existe plusieurs variantes du STC, dont la plus simple (ou plutôt la moins complexe) est le « *Space Time Block Coding* » (STBC), c'est-à-dire « STC par bloc », qui est optionnel en 802.11n. Si l'émetteur a *n* antennes, une information à émettre est d'abord découpée en *n* blocs. Par exemple, avec deux antennes, l'information *x* est d'abord découpée en x_1 et x_2. On émet alors simultanément x_1 sur l'antenne 1 et x_2 sur l'antenne 2. Jusqu'ici, cela ressemble au multiplexage spatial. Mais l'instant d'après (sur le symbole OFDM suivant), on émet à nouveau x_1 et x_2, mais d'une façon transformée et en inversant les antennes : cette fois-ci on émet x_1^* sur l'antenne 2 et $-x_2^*$ sur l'antenne 1. La notation x_1^* désigne une transformation mathématique de x_1 appelée le « conjugué complexe » de x_1 : les propriétés mathématiques du conjugué complexe font que le récepteur a de fortes chances de pouvoir reconstruire correctement *x*, même s'il reçoit mal x_1, x_1^*, x_2 et $-x_2^*$.

2.4 LES CANAUX

Comme nous l'avons vu, toutes les variantes du WiFi découpent la bande de fréquences sur laquelle elles reposent (2,4 GHz ou 5 GHz) en canaux. Ils sont différents selon les variantes utilisées.

2.4.1 Les canaux à 2,4 GHz

Le 802.11 FHSS utilise la bande de 2,4 GHz et la découpe en canaux de 1 MHz numérotés à partir de 2 400 MHz. Les canaux utilisables changent en fonction de la législation du pays où l'on se trouve, mais en deux mots on a droit aux canaux 2 à 83 en Europe et aux canaux 2 à 80 aux États-Unis. Du coup, la plupart des matériels

se limitent aux canaux 2 à 80. Le 802.11 FHSS n'étant presque plus utilisé, nous ne détaillerons pas davantage ses canaux.

Pour toutes les autres variantes du WiFi sur la bande de 2,4 GHz, c'est-à-dire le 802.11 DSSS, le 802.11b, le 802.11g et le 802.11n, quatorze canaux de 22 MHz de largeur sont définis, également numérotés à partir de 2 400 MHz. Leurs centres ne sont espacés que de 5 MHz de sorte qu'ils se superposent en partie. Ceci permet de choisir avec une certaine souplesse la bande de fréquence que l'on préfère utiliser, mais si l'on a deux réseaux au même endroit et qu'ils utilisent des canaux voisins, on aura beaucoup d'interférences. Pour éviter les interférences, on recommande un espace de cinq canaux au moins, donc on ne peut utiliser que trois canaux simultanément au même endroit. Les canaux 1 à 13 sont utilisables en Europe[1], mais en Amérique on ne peut utiliser que les canaux 1 à 11. Quant au canal 14, seul le Japon y a droit. En conséquence, on utilise habituellement les canaux 1, 6 et 11 qui sont suffisamment espacés pour éviter toute interférence et sont autorisés presque partout sur la planète. Au mieux, avec le 802.11g, on peut donc avoir trois points d'accès indépendants au même endroit, offrant chacun un débit théorique de 54 Mb/s soit un total de 162 Mb/s !

Canal	Fréquence basse	Centre	Fréquence haute
1	2 401	2 412	2 423
2	2 406	2 417	2 428
3	2 411	2 422	2 433
4	2 416	2 427	2 438
5	2 421	2 432	2 443
6	2 426	2 437	2 448
7	2 431	2 442	2 453
8	2 436	2 447	2 458
9	2 441	2 452	2 463
10	2 446	2 457	2 468
11	2 451	2 462	2 473
12	2 456	2 467	2 478
13	2 461	2 472	2 483
14	2 473	2 484	2 495

Pour le 802.11 DSSS, le 802.11b, le 802.11g et le 802.11n à 2,4 GHz, 14 canaux de 22 MHz chacun sont définis. Puisqu'ils se superposent, on recommande en général de n'utiliser que les canaux 1, 6 et 11.

1. Voir les tableaux synthétiques concernant la législation du chapitre 11.

2.4.2 Les canaux à 5 GHz

En ce qui concerne le 802.11a et le 802.11n sur la bande de fréquences de 5 GHz, les centres de deux canaux successifs sont également espacés de 5 MHz, mais la numérotation commence à 5 000 MHz. Par exemple, le canal 34 a pour centre 5 170 MHz car 34 × 5 + 5 000 = 5 170. De plus, chaque canal a 20 MHz de largeur, donc le canal 34 s'étend de 5 160 à 5 180 MHz. Naturellement, si l'on souhaite éviter tout chevauchement, il faut utiliser au moins un écart de quatre canaux. Le tableau suivant montre les 19 canaux utilisables actuellement avec le 802.11a et le 802.11n à 5 GHz en Europe. Aux USA, les canaux 100 à 140 sont interdits, mais en revanche, les canaux 149 à 161 sont autorisés.

Canal	Fréquence basse	Centre	Fréquence haute
36	5 170	5 180	5 190
40	5 190	5 200	5 210
44	5 210	5 220	5 230
48	5 230	5 240	5 250
52	5 250	5 260	5 270
56	5 270	5 280	5 290
60	5 290	5 300	5 310
64	5 310	5 320	5 330
100	5 490	5 500	5 510
104	5 510	5 520	5 530
108	5 530	5 540	5 550
112	5 550	5 560	5 570
116	5 570	5 580	5 590
120	5 590	5 600	5 610
124	5 610	5 620	5 630
128	5 630	5 640	5 650
132	5 650	5 660	5 670
136	5 670	5 680	5 690
140	5 690	5 700	5 710

Dans un même lieu, on peut donc avoir jusqu'à 19 points d'accès indépendants, en utilisant ces différents canaux. Cela signifie que l'on peut atteindre un débit total maximal de 1 Gb/s avec le 802.11a ! Dans la pratique, il faut diviser environ par deux ces valeurs, mais cela reste très important. Avec le 802.11n, la capacité théorique à 5 GHz est presque de 3 Gb/s (voir le § 2.6) !

Pour le WiFi à 5 GHz, 19 canaux indépendants de 20 MHz chacun sont utilisables en Europe. Ces couches physiques du WiFi sont donc celles qui offrent la plus grande capacité : jusqu'à 19 fois 54 Mb/s pour le 802.11a, et 19 fois 150 Mb/s pour le 802.11n.

2.4.3 Regroupement de canaux

Certaines solutions propriétaires autorisent depuis plusieurs années le regroupement de deux canaux adjacents pour former un seul canal. Certains AP proposent une liste de couples de canaux adjacents : la bande de fréquences utilisée s'étend alors bien sûr du bas du canal inférieur au haut du canal supérieur. Mais parfois les choses sont moins explicites : on doit choisir un canal principal, puis préciser dans quelle direction on souhaite l'étendre (vers le bas ou le haut du spectre). Par exemple, on peut choisir le canal 36 (qui s'étend normalement de 5 170 MHz à 5 190 MHz) et l'étendre vers le haut (jusqu'à 5 210 MHz). Le double canal de 40 MHz ainsi formé occupe alors la même bande de fréquences que si l'on avait installé deux points d'accès configurés sur une largeur de 20 MHz chacun, l'un sur le canal 36 et l'autre sur le canal 40.

Quel est l'intérêt du regroupement de canaux ? Il est simple : le débit que l'on peut atteindre est proportionnel à la largeur de la bande de fréquences utilisée... le regroupement de deux canaux permet donc de doubler le débit, sans effort.

Puisqu'il s'agissait jusqu'à présent de solutions propriétaires, il fallait que toutes les stations du réseau proviennent du même fournisseur. Mais les choses ont changé depuis l'arrivée du 802.11n en 2006 : les doubles canaux de 40 MHz ont été standardisés, et il est donc possible de profiter d'un double canal de 40 MHz avec des équipements de fournisseurs différents. Le support des doubles canaux de 40 MHz en 802.11n reste toutefois optionnel.

On peut être tenté de systématiquement utiliser un « double canal » de 40 MHz pour doubler le débit, mais il ne faut pas oublier que l'on va alors occuper deux fois plus de spectre radio. Or, celui-ci est limité, surtout pour la bande des 2,4 GHz : on dispose en tout et pour tout en France d'un peu plus de 80 MHz dans cette bande. Si vous déployez un point d'accès à 2,4 GHz sur 40 MHz, vous ne laissez pas beaucoup de place pour les réseaux voisins (notamment pour vos autres points d'accès) et vous risquez donc de subir de fortes interférences. D'ailleurs, bien que le mode 40 MHz sur les canaux à 2,4 GHz soit prévu par le 802.11n, la WiFi Alliance a quant à elle choisi de l'ignorer pour l'instant : ce mode ne fait pas partie des tests d'interopérabilité. Pour résumer, ce mode 40 MHz peut doubler le débit, mais il est surtout recommandé à 5 GHz.

Une station WiFi incompatible avec le regroupement de canaux est incapable de détecter qu'une communication a lieu sur un double canal. Du coup, elle risque de prendre la parole sur l'un des deux canaux alors qu'une station a déjà commencé à émettre sur le double canal : les interférences provoqueront des pertes de paquets à la fois pour elle et pour le réseau à double canal, donc le débit sera réduit et instable. Heureusement, le 802.11n prévoit une solution : avant d'émettre un paquet sur le double canal, une station 802.11n doit d'abord signaler sa volonté d'envoyer un paquet

sur chacun des deux canaux. Les anciennes stations 802.11a/b/g sauront alors qu'il ne faut pas prendre la parole avant un délai précis. La cohabitation entre un réseau classique et un réseau 802.11n sur double canal est donc rendue possible.

2.5 LES TRAMES 802.11

2.5.1 La structure d'une trame

Lorsqu'un paquet de données doit être envoyé sur les ondes, l'adaptateur WiFi commence par le traiter au niveau de la couche MAC (voir le chapitre 3). En bref, le paquet est éventuellement fragmenté et les fragments sont encapsulés dans des paquets appelés des MAC *Protocol Data Unit* (MPDU). La couche physique a donc pour responsabilité de transmettre sur les ondes les MPDU fournis par la couche MAC et inversement de fournir à la couche MAC les paquets reçus sur les ondes.

Au niveau de la couche physique, le MPDU est inclus dans une trame 802.11 dont la structure est la suivante :

Préambule	En-tête PLCP	MPDU

2.5.2 Le préambule

Le préambule permet au récepteur de se synchroniser correctement avec l'émetteur, de s'adapter aux légers décalages de fréquence qui peuvent survenir et éventuellement de choisir l'antenne à utiliser pour la réception, si le récepteur en a plusieurs.

Pour le FHSS, le préambule est composé de deux parties : la première sert à la synchronisation et la seconde indique la fin du préambule et le début de la trame : c'est le *Start Frame Delimiter* (SFD). La synchronisation consiste en une séquence de 80 bits égale tout simplement à 010101...0101. Le SFD est composé de 16 bits : 0000 1100 1011 1101. En notation hexadécimale, cela correspond à 0x0CBD.

Pour le DSSS (802.11 DSSS, 802.11b et 802.11g), le préambule est également composé d'une synchronisation et d'un SFD. La synchronisation est similaire à celle du FHSS, mais il s'agit d'une séquence plus complexe qu'une simple alternance de 0 et de 1. En outre sa longueur est de 128 bits... en tout cas selon la première version du standard 802.11.

Lorsque le 802.11b est arrivé, il a défini un nouveau format optionnel pour la synchronisation, de seulement 56 bits. On parle donc de « préambule court » (*short preamble*). Le but était de gagner un peu de bande passante en raccourcissant le préambule qui est envoyé à chaque paquet. Le gain peut être assez important, pour les débits les plus élevés : en effet, le préambule long peut occuper jusqu'à près de 40 % de la bande passante. Le préambule court n'en occupe plus « que » 20 % environ. Malheureusement, alors que tous les équipements gèrent bien le « préambule long »,

le préambule court est optionnel et en conséquence certains équipements ne savent pas le gérer, même parmi les plus récents. Pour ne rien arranger, certains produits sont configurés avec un préambule court par défaut ! Donc si vous ne comprenez pas pourquoi votre adaptateur ne détecte pas votre point d'accès (AP), vérifiez bien qu'ils utilisent le même préambule : ce sera souvent la réponse à votre problème.

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

Quant au SFD, il s'agit toujours d'une séquence de 16 bits, mais différente du FHSS (0xF3A0).

Pour l'OFDM, le préambule est simplement composé d'une séquence de douze symboles prédéfinis.

2.5.3 L'en-tête PLCP

L'en-tête *Physical Layer Convergence Procedure* (PLCP) contient des informations importantes pour que le récepteur puisse se préparer à la réception du MPDU. En particulier, la longueur de la trame et la vitesse de transfert à utiliser sont indiquées. L'en-tête PLCP est toujours transmis à 1 Mb/s, quelle que soit la couche physique utilisée et le débit peut augmenter pour la transmission du MPDU.

Pour le FHSS, l'en-tête est composé de trois champs :

Longueur	Débit	Contrôle d'erreur
12 bits	4 bits	16 bits

- la longueur de la trame est indiquée en nombre d'octets (1 octet = 8 bits) ;
- le débit peut être de 1 ou de 2 Mb/s, comme nous l'avons vu ;
- le champ de contrôle d'erreur s'appelle le *Header Error Check* (HEC) : il est calculé à partir des deux champs précédents selon un algorithme appelé le Contrôle de redondance cyclique (CRC). Le récepteur peut effectuer le même calcul à l'arrivée et s'assurer qu'il obtient bien le même résultat : dans le cas contraire, il sait qu'une erreur de transmission a eu lieu.

Les en-têtes PLCP du DSSS et de l'OFDM ont un format semblable à celui du FHSS, avec quelques champs supplémentaires sans grande importance et plus de bits pour les champs de longueur et de débit. L'en-tête PLCP de l'OFDM n'a pas de champ HEC, mais à la place un simple bit de parité, égal à 0 si le nombre de 1 dans les champs débit et longueur est pair.

2.6 LA NORME 802.11N

2.6.1 La norme 802.11n et ses « drafts »

Après le 802.11a, le 802.11b et le 802.11g, les performances du WiFi se sont encore améliorées en 2006 avec la publication de la première ébauche (*draft* 1.0) du standard 802.11n. Le *draft* 2.0 a été publié peu après, en 2007, et l'on attendait la version définitive dans la foulée, mais sa publication a été retardée à plusieurs reprises, et elle est maintenant prévue pour janvier 2010. Néanmoins, le *draft* 2.0 est assez détaillé, et les constructeurs se sont donc lancés sans plus attendre dans l'aventure du « 11n » : de nombreux produits respectant le *draft* 2.0 sont ainsi apparus sur le marché. D'abord très chers, ces produits se sont petit à petit démocratisés, et de nombreux ordinateurs portables grand public sont maintenant vendus avec un adaptateur 802.11b/g/n intégré (ou parfois 802.11a/b/g/n). À terme, il devrait petit à petit dominer le marché.

Certaines entreprises ont hésité à investir dans du matériel « 802.11n *draft* 2.0 » de peur qu'il faille le changer au moment de la publication de la norme 802.11n définitive. Ce scénario catastrophe semble peu probable car les spécifications matérielles du 802.11n ont été figées par le groupe de travail de l'IEEE en 2007 : une simple mise à jour du micrologiciel (*firmware*) devrait donc suffire pour transformer un équipement « 802.11n *draft* 2.0 » en équipement « 802.11n » tout court.

> **Attention** : certains produits se disent « WiFi pré-n » ou « WiFi MIMO », il faut bien s'assurer qu'ils respectent le 802.11n ou le *draft* 2.0 du 802.11n, car il s'agit parfois de solutions WiFi mettant en œuvre des techniques MIMO de façon propriétaire.

2.6.2 Un meilleur débit et une plus grande portée

Le 802.11n a connu le succès depuis la publication de ses premières ébauches, avant même sa ratification. Pourquoi un tel engouement? D'abord parce qu'il promet d'étendre de 10 à 20 % la portée du WiFi. Mais surtout parce qu'il promet un débit exceptionnel, en théorie jusqu'à 600 Mb/s en MIMO 4 × 4 × 4 (voir § 2.3.6) sur un double canal de 40 MHz, et avec toutes les fonctions d'optimisation activées (voir ci-après). Cela représente plus de 10 fois le débit du 802.11a ou du 802.11g. Toutefois, ce débit n'existe pour l'instant que sur le papier, car l'état de l'art en 2009 n'offrait au mieux, dans des conditions idéales, « que » 450 Mb/s en MIMO 3 × 3 × 3. Dans la pratique, il est plus raisonnable d'espérer au mieux un débit théorique de 300 Mb/s sur un double canal de 40 MHz, ou 150 Mb/s sur un canal classique de 20 MHz[1]. Rappelons que le débit théorique correspond au débit maximal mesuré au niveau de la couche physique : le débit réel, c'est-à-dire celui observé par l'utilisateur, lorsqu'il transfère un fichier par exemple, est généralement de l'ordre de la moitié ou du tiers du débit théorique. On peut donc espérer aujourd'hui obtenir avec le 802.11n un débit

1. La liste des débits théoriques prévus par le 802.11n en fonction de la distance (maximale) est résumée sur la figure 2.5. On multipliera ce débit par le nombre de flux MIMO, et par deux si l'on utilise un double canal.

réel maximal, en conditions parfaites, d'environ 130 Mb/s. Cela reste bien meilleur que les 20 à 25 Mb/s réels offerts par le 802.11a et le 802.11g.

Contrairement à ses prédécesseurs, le 802.11n peut fonctionner sur l'une ou l'autre des bandes de fréquences autorisées pour le WiFi : 2,4 GHz ou 5 GHz. Il est d'ailleurs compatible avec toutes les variantes antérieures du WiFi : le 802.11b et le 802.11g à 2,4 GHz et le 802.11a à 5 GHz. Malheureusement, les produits 802.11n sont souvent simple bande, généralement à 2,4 GHz (pour des raisons de coût de production). Les équipements simple bande à 2,4 GHz peuvent être certifiés par la WiFi Alliance (il est d'ailleurs conseillé de n'acheter que des produits certifiés), et ils obtiennent alors le label « WiFi b/g/n » (ou « WiFi a/n »), tandis que les équipements double bande obtiennent le label « WiFi a/b/g/n » dont le logo est représenté sur la figure 2.18.

Figure 2.18 — Logo pour les produits certifiés WiFi a/b/g et n *draft* 2.0.

2.6.3 Les principales améliorations du 802.11n

Comment le 802.11n parvient-il à augmenter la portée et doper le débit? D'abord par de considérables améliorations au niveau de la couche physique :

- l'utilisation de plusieurs techniques MIMO (voir § 2.3.6) : le codage espace-temps permet en principe d'augmenter la portée du signal de 10 à 20 %, tandis que le multiplexage spatial peut aller jusqu'à quadrupler le débit maximal (en MIMO 4 × 4 × 4), selon les conditions radio ;
- le regroupement de canaux (optionnel) afin d'utiliser une bande de 40 MHz de largeur plutôt que 20 MHz habituellement : ceci permet de doubler le débit ;
- d'autres améliorations plus légères qui peuvent chacune améliorer le débit de 10 % environ :
  - 52 sous-porteuses OFDM plutôt que 48 ;
  - un délai de garde plus court entre les symboles OFDM, de 400 ns plutôt que 800 ns (optionnel) ;
  - un préambule plus court (optionnel).

D'autre part, des améliorations de la couche MAC peuvent encore doubler le débit, selon le type de trafic émis (nous approfondirons ces points au prochain chapitre) :

- l'agrégation de paquets afin de remplir au maximum les trames envoyées sur les ondes ;
- l'utilisation d'acquittements groupés (« *block-ACK* »).

Résumé

Afin de présenter en détail les couches physiques du WiFi, nous avons commencé par quelques rappels sur les ondes radio : les grandeurs physiques qui caractérisent une onde électromagnétique (fréquence, puissance...), le rapport signal/bruit (RSB), la notion de « multipath », etc.

Dans un deuxième temps, nous avons présenté les modulations analogiques les plus simples (AM, FM et PM). Ceci nous a permis d'attaquer ensuite les modulations numériques correspondantes : ASK, FSK et PSK. Quelques variantes de ces modulations ont été présentées, du FSK Gaussien (GFSK) aux modulations différentielles (DPSK...). Nous avons ensuite montré que plusieurs bits d'information peuvent être transmis dans un seul signal radio, qu'on appelle un « symbole ». Ceci nous a permis de présenter des modulations plus complexes telles que le 8FSK ou encore le QAM.

Forts de ces bases, nous avons étudié les trois principales modulations utilisées par les couches physiques du 802.11 : le FHSS, le DSSS et l'OFDM.

Le FHSS fonctionne en sautant rapidement d'un canal à un autre : il offre un débit limité mais une capacité importante et une bonne résistance au bruit, si celui-ci est localisé dans le spectre. Il n'est plus beaucoup utilisé en WiFi.

Le DSSS repose sur une technique de « *chipping* » permettant d'offrir une redondance importante et d'étaler le signal sur un spectre large. Il offre un débit plus important (jusqu'à 11 Mb/s avec le HR-DSSS), une meilleure portée et une bonne résistance au bruit « blanc » réparti de façon homogène dans le spectre. En revanche, il est plus sensible au bruit localisé.

L'OFDM est une modulation radio très sophistiquée offrant un excellent débit. Elle divise le canal radio en de multiples sous-porteuses et émet simultanément une portion des données sur chacune d'entre elles. Les porteuses sont « orthogonales » de sorte qu'elles ne se gênent pas (peu d'interférences ICI). Chaque symbole transporte ainsi de très nombreux bits, de sorte qu'il est possible de les espacer dans le temps tout en conservant un débit important : ceci permet de limiter les effets du multipath. Enfin, des codes correcteurs d'erreurs permettent de bénéficier d'une excellente résistance au bruit.

Nous avons également présenté quatre techniques multi-antennes fréquemment exploitées dans des produits WiFi :

– la diversité d'espace permettant au récepteur de mieux résister aux interférences dues aux multiples chemins empruntés par les ondes (le *multipath*) ;

– le *beamforming*, permettant à l'émetteur de focaliser automatiquement le signal qu'il émet en direction du récepteur, afin d'en augmenter la portée et de limiter les interférences avec les réseaux voisins ;

– le multiplexage spatial, permettant de démultiplier le débit en envoyant simultanément une partie de l'information sur chaque antenne – plus le *multipath* est important, plus les canaux spatiaux ainsi obtenus sont exploitables pour que le récepteur distingue les différents flux émis, mais il faut autant d'antennes du côté de l'émetteur que du côté de l'émetteur ;

– le codage espace-temps, qui permet d'améliorer le rapport signal/bruit (donc la

portée du signal) en envoyant les informations de façon redondante dans le temps et dans l'espace.

Le 802.11a se situe à 5 GHz et repose sur l'OFDM. Il peut atteindre 54 Mb/s. Le 802.11b se situe à 2,4 GHz et utilise le DSSS ou le HR-DSSS pour les plus hauts débits (11 Mb/s). Le 802.11g se situe à 2,4 GHz et repose sur le DSSS, le HR-DSSS ou l'OFDM, en changeant automatiquement. Avec l'OFDM, il peut monter à 54 Mb/s. La bande de fréquences de 2,4 GHz est divisée, pour le DSSS ou l'OFDM, en quatorze canaux de 22 MHz chacun, qui se superposent de sorte que seuls trois canaux indépendants peuvent être utilisés simultanément (les canaux 1, 6 et 11 sont souvent choisis). La bande de fréquences de 5 GHz est divisée en 19 canaux indépendants de 20 MHz chacun. La capacité totale du 802.11a est donc importante car on peut installer 19 points d'accès à 54 Mb/s au même endroit offrant chacun 54Mb/s, soit en théorie plus de 1 Gb/s.

Nous avons ensuite présenté les trames 802.11. Elles sont composées de trois parties : un préambule, un en-tête PLCP et un MPDU. Le préambule permet au récepteur de se préparer à la réception. En DSSS, il peut être court ou long, sachant que le court n'est pas toujours géré. L'en-tête PLCP indique la longueur de la trame et le débit à utiliser pour la suite de la transmission. L'en-tête lui-même est toujours envoyé au plus bas débit. Le MPDU est le paquet que la couche MAC souhaite envoyer, comme nous allons le voir au chapitre 3.

Pour finir, nous avons présenté le 802.11n. La première ébauche du 802.11n est parue en 2006, la seconde (le *draft* 2.0) en 2007 et la norme définitive doit être publiée en janvier 2010. Il est compatible à la fois avec les normes 802.11b/g à 2,4 GHz, et avec le 802.11a à 5 GHz, mais beaucoup d'équipements 802.11n ne sont malheureusement compatibles qu'avec l'une des deux bandes (généralement à 2,4 GHz). Le 802.11n repose sur l'OFDM, comme le 802.11a et le 802.11g. Il met en œuvre plusieurs techniques avancées qui permettent d'améliorer le débit et la portée du WiFi : notamment des techniques MIMO et MISO (multiplexage spatial et codage espace-temps), le regroupement optionnel de deux canaux adjacents pour former un double canal de 40 MHz, et quelques optimisations de la couche MAC. Le débit théorique maximal qu'il peut atteindre est de 600 Mb/s, en conditions parfaites, avec du MIMO $4 \times 4 \times 4$, sur un double canal de 40 MHz et avec toutes les optimisations possibles activées. Dans la pratique, on peut espérer plutôt environ 300 Mb/s. Sur un canal simple de 20 MHz, on peut espérer 150 Mb/s. À 5 GHz, avec 19 canaux indépendants, en conditions idéales, la capacité du 802.11n peut donc atteindre près de 3 Gb/s, soit trois fois plus que le 802.11a.

3

La norme 802.11 : couche MAC

Objectif

Au cours du chapitre précédent, nous avons présenté les couches physiques définies par le standard 802.11. Nous allons maintenant aborder la couche de contrôle d'accès au média (*Medium Access Control*, MAC) qui a un rôle crucial : elle définit comment différents utilisateurs doivent se partager la parole, le format des paquets échangés, les topologies possibles, les modalités exactes de connexion à un réseau sans fil (on parle « d'association ») et elle va même plus loin en définissant des fonctionnalités avancées telles que la sécurité des communications, l'économie d'énergie, le contrôle d'erreur ou encore comment assurer une bonne qualité de service, en particulier pour les communications multimédias. La couche MAC est donc en quelque sorte le « cerveau » du WiFi.

3.1 TOUR D'HORIZON DE LA COUCHE MAC

3.1.1 Les couches LLC et MAC

Lorsque nous avons présenté le modèle OSI, au cours du premier chapitre, nous n'avions pas parlé de la couche MAC. En réalité, le modèle OSI n'est pas mis en œuvre tel quel dans la pratique : les couches se recoupent partiellement, certaines sont regroupées en une seule et d'autres sont divisées en plusieurs. Les couches physiques du WiFi, dont nous avons parlé au chapitre 2, correspondent bien à la première couche du modèle OSI. En revanche, la couche MAC correspond à la partie « basse » de la

deuxième couche OSI, la couche de « liaison de données ». En effet, l'IEEE a divisé cette couche en deux couches superposées : « en haut » se trouve la couche de contrôle de la liaison logique (*Logical Link Control*, LLC) et « en bas » la couche de contrôle d'accès au support (MAC).

La couche LLC est standardisée par l'IEEE sous le nom 802.2 depuis le début des années 1980. Son but est de permettre aux protocoles réseaux de niveau 3 (par exemple IP) de reposer sur une couche unique (la couche LLC) quel que soit le protocole sous-jacent utilisé, dont le WiFi, l'Ethernet ou le Token Ring, par exemple. Tous les paquets de données WiFi transportent donc un paquet LLC, qui contient lui-même des paquets issus des couches réseaux supérieures. L'en-tête d'un paquet LLC indique le type du protocole de niveau 3 qu'il contient : la plupart du temps, il s'agit du protocole IP, mais cela pourrait être un autre protocole, comme IPX (*Internet Packet Exchange*) par exemple. Grâce à la couche LLC, il est possible d'avoir en même temps, sur un même réseau, plusieurs protocoles de niveau 3.

Figure 3.1 — Les couches réseaux.

3.1.2 Les fonctions de la couche MAC

De son côté, la couche MAC est, comme nous l'avons dit en introduction, le « cerveau » du WiFi. La première version du standard 802.11 (le *802.11legacy*, publié en 1997), a défini la couche MAC en y intégrant un certain nombre de fonctionnalités cruciales, telles que le partage de la parole entre utilisateurs, les modalités de connexion au réseau, le contrôle d'erreur ou encore la sécurité, que nous détaillerons au cours de ce chapitre.

La couche MAC définit également les adresses du réseau : tous les périphériques possèdent un identifiant de 48 bits (6 octets) connu sous le nom « d'adresse MAC ». Les trois premiers octets désignent le fabricant du matériel réseau. Par exemple, en notation hexadécimale, 00-00-0C correspond au constructeur Cisco, 00-04-23 correspond à Intel Corporation, etc. Les trois octets suivants définissent un identifiant

unique choisi par le fabricant, par exemple 8B-B5-0B. Une adresse ressemblera donc par exemple à : 00-04-23-8B-B5-0B. Tout adaptateur réseau (WiFi, Ethernet ou autre) possède donc en principe une adresse MAC, censée être unique au monde. On peut communiquer avec un périphérique en envoyant des paquets sur le réseau, libellés à son adresse MAC.

Les autres protocoles standardisés par l'IEEE, tels que l'Ethernet ou le *Token Ring*, possèdent la même définition de l'adresse MAC. Ceci permet à des stations situées sur des réseaux de types différents de pouvoir communiquer entre elles : il suffit pour cela de connecter les différents réseaux entre eux avec des « ponts » (*bridge*). De nombreux aspects de la couche MAC du WiFi sont inspirés directement de la couche MAC de l'Ethernet, comme nous le verrons plus loin, au point que certains désignent le WiFi sous le nom « d'Ethernet sans fil ».

3.1.3 Les évolutions de la couche MAC

La couche MAC de la première version du standard 802.11 est encore d'actualité et l'essentiel de ce chapitre porte sur les fonctionnalités de la couche MAC présentes depuis le début. Toutefois, de nombreuses améliorations ont été apportées à cette couche MAC, au fil du temps. En voici une présentation rapide :

- **Le 802.11c** – Il apporte quelques précisions sur le fonctionnement d'un AP (Access Point) connecté à un réseau filaire. Ces précisions sont surtout utiles pour les constructeurs de matériel WiFi et il n'est pas nécessaire de s'en soucier davantage.
- **Le 802.11d** – Il établit la liste des règles à suivre selon les pays pour pouvoir émettre sur telle ou telle fréquence : éviter tel ou tel canal, limiter la puissance, etc. Le 802.11d permet ainsi aux constructeurs de savoir facilement comment configurer leurs produits en fonction des pays auxquels ils sont destinés.
  Certains produits sont configurés pour un pays donné, dès la fabrication. D'autres produits demandent à l'utilisateur de préciser le pays dans lequel il se trouve. Le produit est alors configuré dynamiquement. Malheureusement, certains constructeurs ont du retard sur les évolutions de la législation française : jusqu'en 2002, seuls les canaux 10 à 13 étaient autorisés en France pour le 802.11b et le 802.11g. L'ARCEP a libéré les canaux 1 à 9 fin 2002, mais de nombreux constructeurs ont continué, pendant presque deux ans, à fournir des produits bridés !
- **Le 802.11e** – Ratifié fin 2005, il définit des mécanismes permettant de mieux contrôler le flux de données et le partage du média entre plusieurs stations : ceci permet notamment de mettre en œuvre une véritable gestion de la qualité de service (*Quality of Service*, QoS) pour permettre l'échange fluide de données multimédias. Nous y reviendrons en détail au § 3.2.3.
- **Le 802.11F** – Il définit le protocole interpoints d'accès (*Inter Access Point Protocol*, IAPP) : celui-ci précise comment des points d'accès (bornes WiFi) d'un même réseau sans fil doivent communiquer entre eux. L'IAPP permet de constituer un réseau sans fil à partir d'AP de différents constructeurs. Les AP

ont souvent besoin de communiquer entre eux, notamment pour permettre le *hand-over*[1], c'est-à-dire la possibilité pour un utilisateur de passer, sans déconnexion, d'un AP à un autre au sein d'un même réseau sans fil.
Si vous prévoyez que votre réseau sans fil sera constitué d'AP de différents constructeurs, assurez-vous qu'ils soient au moins certifiés WiFi par la WiFi Alliance : comme celle-ci effectue des tests d' interopérabilité, il n'est pas rare que des AP ayant reçu ce label fonctionnent bien ensemble, même s'ils proviennent de différents constructeurs. Mais rien n'est garanti. Pour être assuré d'une bonne interopérabilité entre AP, recherchez les AP mettant en œuvre le 802.11F.

- **Le 802.11h** – Il apporte des modifications à la couche physique 802.11a ainsi qu'à la couche MAC, afin de mieux adapter le WiFi au marché européen[2]. En effet, le mode de fonctionnement du WiFi rentre en conflit avec certaines communications satellites pour la bande de fréquences de 5 GHz. Pour éviter ce conflit, le 802.11h met en œuvre un mécanisme de contrôle de la puissance de transmission (*Transmit Power Control*, TPC) dynamique, qui consiste à ne jamais émettre plus fort que nécessaire, tout en restant assez fort pour que le récepteur puisse capter le signal. En outre, si un canal est occupé par une communication radio non WiFi, le 802.11h spécifie comment changer dynamiquement de canal : ce mécanisme s'appelle la sélection dynamique de fréquence (*Dynamic Frequency Selection*, DFS). Le 802.11h a été validé en septembre 2003.
- **Le 802.11i** – La solution de sécurité offerte par la première version de la couche MAC s'appelle le *Wired Equivalent Privacy* (WEP). Nous l'approfondirons au chapitre 7 et nous verrons qu'elle possède de très nombreuses failles : un réseau protégé par le WEP est très vulnérable à des attaques de pirates informatiques. Le 802.11i a été ratifié le 24 juin 2004 et il apporte une solution nettement plus sûre et flexible que le WEP. Nous y reviendrons en détail dans les chapitres 6 à 10.
- **Le 802.11j** – Il est au Japon ce que le 802.11h est à l'Europe : il définit une série de mécanismes pour adapter le 802.11a à la législation du Japon.
- **Le 802.11k** – Il définit un certain nombre de paramètres radio et de statistiques qui peuvent être échangés entre équipements WiFi ou présentés à un utilisateur. Par exemple, avec le 802.11k, les stations établissent régulièrement la liste des équipements WiFi situés près d'elles. Un AP peut alors demander à une station de lui envoyer sa liste et il peut utiliser cette liste afin d'estimer si la station ferait mieux de se connecter à un autre AP.
  Par ailleurs, le 802.11k définit comment un AP peut envoyer à intervalles réguliers (dans les trames balises, que nous verrons au § 3.4.1) un rapport sur son environnement radio. Cette information peut être utilisée par une station pour choisir le meilleur AP auquel se connecter.

1. To *hand-over* signifie « passer la main ». Certains parlent également de *roaming* ou « d'itinérance », mais ceci peut entraîner des confusions avec le *roaming* entre WISP, qui permet à un abonné du WISP X de se connecter à un *hotspot* du WISP Y (voir le chapitre 1).
2. Voir les tableaux synthétiques concernant la législation du chapitre 11.

Le 802.11k permet une supervision détaillée du réseau, par exemple pour visualiser un histogramme du niveau du bruit au cours du temps.
Enfin, grâce aux échanges d'informations concernant l'environnement radio, le 802.11k facilite la mise en œuvre d'un contrôle de puissance d'émission, ce qui peut améliorer l'environnement radio et diminuer la consommation électrique des équipements.

- **Le 802.11s** – Pour les réseaux maillés (voir § 3.3.2).

Conclusion – Tous les équipements WiFi mettent en œuvre, au minimum, la première version de la couche MAC et certains équipements complètent cette couche avec quelques-unes des améliorations plus récentes. Il est donc important de vérifier les fonctionnalités exactes d'un produit avant l'achat, tout en sachant que certaines fonctionnalités peuvent être rajoutées *a posteriori* par une simple mise à jour du microprogramme (*firmware*) de l'équipement.

3.1.4 Un rappel sur l'Ethernet

Les standards Ethernet

Le WiFi a été conçu, nous l'avons dit, comme une version sans fil du protocole Ethernet. Les deux se marient d'ailleurs très bien. Si vous avez déjà monté un réseau Ethernet, vous n'aurez aucune difficulté à comprendre et à mettre en œuvre votre premier réseau WiFi. On y retrouve dans une grande mesure les mêmes notions et les mêmes outils. Pour aborder la couche MAC du WiFi, nous allons donc commencer par une brève présentation de l'Ethernet et de sa couche MAC.

L'Ethernet a été conçu sur plusieurs années au début des années 1970 par un groupe de chercheurs au sein de la société *Xerox Palo Alto Research Center* (Xerox PARC), dont en particulier Robert Metcalfe (qui fonda par la suite la société 3Com). Le but du projet de recherche était de connecter en réseau des ordinateurs et des imprimantes laser. Xerox Corporation déposa un brevet sur cette technologie fin 1977. En 1979, les sociétés *Digital Equipment Corporation* (DEC), Intel et Xerox s'unirent pour améliorer l'Ethernet et publièrent ensemble le premier standard en 1980 : l'*Ethernet Blue Book* parfois appelé DIX (d'après les initiales des trois compagnies). Pour finir, l'IEEE standardisa cette technologie en 1983 : le 802.3 était né... bien avant le 802.11 ! Un peu par abus de langage, ce standard 802.3 est appelé Ethernet. Le format des paquets Ethernet DIX est légèrement différent de celui des paquets Ethernet 802.3, mais les deux peuvent coexister sur un même réseau.

Une zone de diffusion

L'Ethernet permet aux stations d'un réseau de communiquer en s'échangeant des paquets de données de petite taille (d'environ 1 500 octets en général). Pour cela, les ordinateurs doivent être connectés les uns aux autres avec des câbles – en général de cuivre ou de fibre optique – soit directement entre eux, soit par le biais d'équipements chargés de diffuser les communications au sein du réseau : des « répétiteurs » ou des « concentrateurs » (également appelés multirépétiteurs ou *hub*). Lorsqu'un ordinateur

émet un paquet de données Ethernet, tous les ordinateurs du réseau le reçoivent car ils partagent le même média de communication.

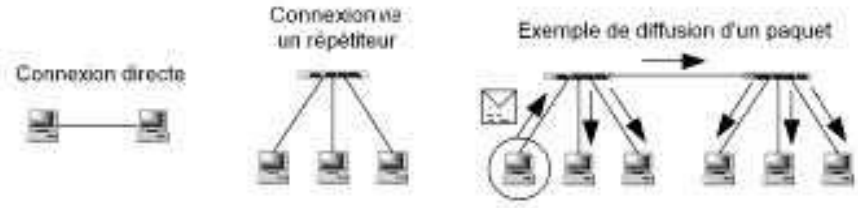


Figure 3.2 — Exemple de réseaux Ethernet et diffusion des paquets.

On peut comparer ceci à un groupe de personnes dans une même salle de réunion : lorsqu'une personne parle, tout le monde l'entend : c'est une zone de diffusion, avec les avantages et les inconvénients que cela représente. L'avantage principal est la simplicité et la performance lorsque le nombre de stations est limité. L'inconvénient est le risque de cacophonie lorsque de nombreuses stations cherchent à communiquer en même temps. En outre, ce modèle pose un problème de sécurité important : il suffit à un pirate de se connecter au support de communication pour pouvoir capter tout le trafic réseau ! Et rien n'empêche à ce pirate de faire une attaque de type « déni de service » (*Denial of Service*, DoS) en saturant le réseau avec des paquets inutiles : tout le monde reçoit alors ces paquets et la bande passante est monopolisée par le pirate.

Unicast, broadcast, multicast

Un paquet peut être adressé à une station en particulier, qui est repérée par son adresse MAC (par exemple, 00:04:23:8D:B5:0B). On parle alors d'*unicast*. Dans ce cas, seule la machine intéressée prend le paquet en compte : en réalité, les autres stations le reçoivent également, mais elles sont censées l'ignorer. Certains adaptateurs réseau possèdent un mode promiscuité (*promiscuous*) qui permet à un logiciel de lire tous les paquets, même ceux qui devraient être ignorés : ce mode est utile pour analyser précisément (sniffer) ce qui se passe sur le réseau, dans le but d'en améliorer les performances ou pour trouver la source d'un problème. Les pirates apprécient ce mode qui leur permet d'espionner toutes les communications.

Par ailleurs, chaque paquet de données peut être adressé explicitement à tout le monde : on parle alors de *broadcast* (c'est-à-dire « émission » ou « diffusion »). Pour cela, le paquet doit être envoyé à l'adresse MAC FF:FF:FF:FF:FF:FF. Ceci offre trois possibilités importantes :

- cela permet de demander un service sans qu'il soit nécessaire de savoir qui y répondra (voir le protocole DHCP) ;
- cela permet de découvrir automatiquement des informations sur les stations reliées au réseau (nous verrons un exemple avec le protocole ARP) ;
- d'autre part, lorsque de nombreuses stations sont intéressées par les données émises (par exemple si plusieurs personnes regardent la même vidéoconférence),

on peut envoyer les données en une seule fois plutôt que d'en faire une copie par destinataire. On économise ainsi de la bande passante.

Pour finir, un paquet peut être adressé à un groupe de stations, grâce à certaines adresses MAC particulières destinées à cet effet (par exemple : 01:00:5E:00:00:01). Toutes les stations intéressées par le trafic de ce type le prendront en compte, les autres l'ignoreront. On parle alors de *multicast*. L'un des intérêts du multicast est, comme pour le broadcast, l'optimisation de la bande passante lorsqu'un même flux de données doit être acheminé vers plusieurs destinataires. Mais alors qu'un paquet broadcast est non discriminatoire et toutes les stations sont censées le prendre en compte, un paquet multicast n'est pris en compte que par les stations qui ont choisi d'appartenir au groupe auquel il est destiné. Le broadcast peut être vu comme un cas particulier de multicast.

Le CSMA

Avec l'Ethernet, chaque équipement attend qu'il y ait un silence pour « prendre la parole », c'est-à-dire pour émettre un paquet de données. C'est ce qu'on appelle l'algorithme *Carrier Sense Multiple Access* (CSMA) : littéralement, on pourrait traduire ceci par « accès multiple avec écoute du média de communication ». En d'autres termes, une station qui souhaite communiquer « écoute » d'abord sur le média de communication et attend un « silence » d'une durée prédéfinie (appelé le *Distributed Inter Frame Space* ou DIFS). Une fois ce délai obligatoire écoulé, la station commence un compte à rebours d'une durée aléatoire. La durée maximale de ce compte à rebours s'appelle la fenêtre de collision (*Collision Window*, CW). Si aucun équipement ne prend la parole avant la fin du compte à rebours, la station émet simplement son paquet. En revanche, si elle se fait doubler par une autre station, elle arrête immédiatement son compte à rebours et attend le prochain silence. Ensuite, elle poursuit son compte à rebours là où elle l'avait laissé. Ceci est résumé sur la figure 3.3. Le délai d'attente aléatoire a pour intérêt de permettre une distribution statistiquement équitable du temps de parole entre les différents équipements du réseau, tout en rendant peu probable (mais pas impossible) le fait que deux équipements prennent la parole exactement en même temps. Le système de compte à rebours permet d'éviter qu'une station attende trop longtemps avant d'émettre son paquet. C'est un peu ce qui se passe dans une salle de réunion lorsqu'il n'y a pas de maître de séance (et que tout le monde est poli) : on attend un silence, puis encore quelques instants avant de parler, pour laisser le temps à quelqu'un d'autre de prendre la parole. Le temps de parole est ainsi réparti aléatoirement, c'est-à-dire plus ou moins équitablement.

Ce protocole est très simple à mettre en œuvre et il est assez performant quand il y a relativement peu d'équipements cherchant à communiquer en même temps : chacun peut « s'exprimer » sans ordre particulier et être entendu par tout le monde. Malheureusement, il perd toute son efficacité lorsque le nombre de machines actives augmente car il arrive alors fréquemment que deux machines prennent la parole en même temps, ce qu'on appelle une « collision ». Dans ce cas, les paquets émis en même temps se superposent et sont donc incompréhensibles : c'est la cacophonie.

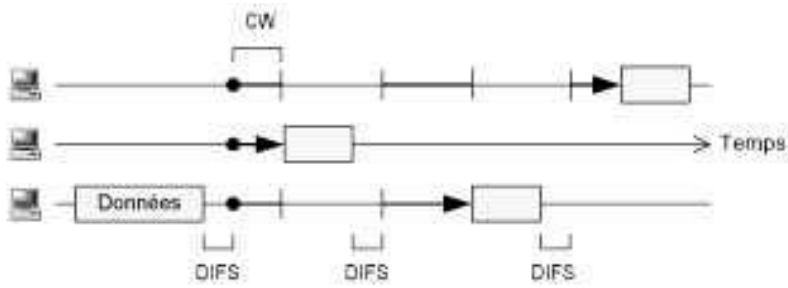


Figure 3.3 — Le partage du temps de parole avec la méthode CSMA.

Le CSMA/CD

Pour diminuer l'impact des collisions sur les performances du réseau, l'Ethernet utilise un algorithme appelé *CSMA with Collision Detection* (CSMA/CD) : lorsqu'un équipement émet un paquet, il écoute en même temps sur le média de communication pour s'assurer qu'il n'y ait pas de collision avec un paquet émis par une autre station. En cas de collision, l'émetteur annule immédiatement l'envoi du paquet. Ceci permet de limiter la durée des collisions : on ne perd pas de temps à envoyer un paquet complet si l'on détecte une collision. Après une collision, l'émetteur attend à nouveau le silence et encore une fois, il poursuit son attente pendant une durée aléatoire ; mais cette fois-ci cette durée aléatoire est proche du double de la précédente : c'est ce qu'on appelle le *back-off* (c'est-à-dire le « recul ») exponentiel. En fait, la fenêtre de collision est simplement doublée (sauf si elle a déjà atteint une durée maximale). Dès qu'un paquet est émis correctement, la fenêtre revient à sa taille initiale.

Encore une fois, c'est ce que l'on fait naturellement dans une salle de réunion : si plusieurs personnes prennent la parole exactement en même temps, elles s'en rendent compte immédiatement (car elles écoutent en même temps qu'elles parlent) et elles s'interrompent sans terminer leur phrase. Après quelques instants, l'une d'entre elles reprend la parole. Si une nouvelle collision a lieu, les deux s'interrompent à nouveau et ont tendance à attendre un peu plus longtemps avant de reprendre la parole.

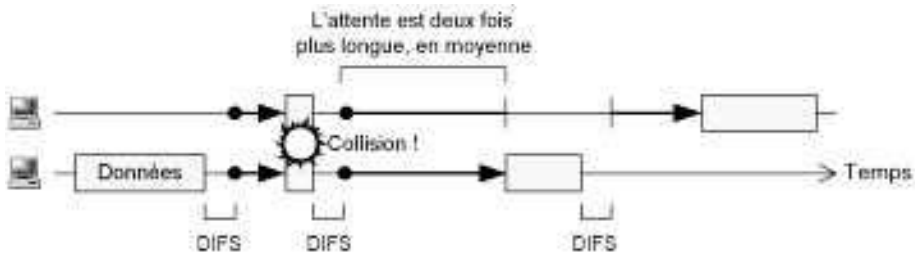


Figure 3.4 — La gestion des collisions avec le CSMA/CD.

3.2 LE PARTAGE DES ONDES EN WIFI

Le WiFi possède des points communs importants avec l'Ethernet :

- chaque paquet peut être adressé à une station, à plusieurs stations ou à toutes les stations (*unicast*, *multicast* ou *broadcast*) ;
- les stations partagent toutes un même média de communication : les câbles réseau pour l'Ethernet, les ondes radio pour le WiFi ;
- toute personne ayant accès au média de communication peut « sniffer » le trafic réseau s'il possède un adaptateur WiFi possédant le mode *promiscuous*.

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

3.2.1 Le mode DCF

La première stratégie s'appelle la fonction de coordination distribuée (*Distributed Coordination Function*, DCF). Il s'agit d'une version améliorée du protocole CSMA *with Collision Avoidance* (CSMA/CA), qui est elle-même une variante du CSMA/CD. Avec le CSMA/CA, lorsqu'une station émet un paquet (en suivant la logique CSMA), elle attend en retour un accusé de réception (ou *acknowledgment*, noté ACK). Celui-ci a pour but de s'assurer que le paquet est bien arrivé à destination et qu'aucune collision n'a eu lieu. Le mode DCF du 802.11 repose sur ce principe avec quelques éléments supplémentaires.

Avant d'émettre un paquet de données, en mode DCF, la station WiFi attend un silence radio d'une durée prédéfinie (le *Distributed Inter Frame Space*, DIFS), suivi d'un délai d'attente supplémentaire aléatoire. Pour l'instant, rien de neuf. Mais ensuite, au lieu d'émettre un paquet de données, la station envoie un minuscule paquet dénommé *Request To Send* (RTS), c'est-à-dire « demande la permission d'envoyer un paquet ». Ce paquet indique, entre autres, une estimation du temps que prendra l'émission du paquet de données. La station réceptrice renvoie alors aussitôt un paquet *Clear To Send* (CTS) pour donner son autorisation à la station émettrice. En répondant après un très bref délai appelé le *Short Inter Frame Space* (SIFS), bien inférieur au DIFS, on est assuré qu'aucune autre station n'aura la mauvaise idée d'envoyer un paquet entre le RTS et le CTS. Le CTS contient lui aussi la durée estimée d'émission du paquet de données afin de prévenir toutes les autres stations à proximité qu'un paquet de données va être envoyé et qu'elles doivent donc attendre pendant la durée indiquée avant de tenter de prendre la parole.

Une fois le CTS reçu, la station émettrice attend un bref délai (SIFS) et envoie son paquet de données. Une fois ce paquet correctement reçu et encore après un délai SIFS, la station réceptrice renvoie un ACK. Celui-ci a pour but d'assurer à l'émetteur que le paquet est bien arrivé et qu'aucune collision n'a eu lieu.

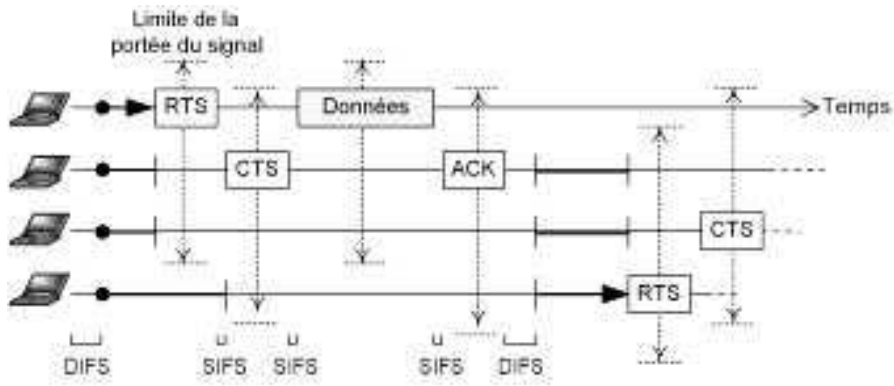


Figure 3.5 — Les mécanismes CSMA/CA et RTS/CTS.

Notons que ce mécanisme n'est valable que pour le trafic unicast : les paquets de broadcast ou de multicast sont envoyés sans RTS, sans CTS et sans ACK. *Attention* : lorsqu'une station est connectée à un AP (mode Infrastructure, voir § 3.3) et qu'elle émet un paquet en broadcast ou multicast, elle l'envoie en réalité uniquement à cet AP, selon le principe unicast. L'AP se charge ensuite de relayer le paquet à ses destinataires, en broadcast ou multicast.

Avec le mécanisme RTS/CTS, on peut éviter la majorité des collisions plutôt que de les détecter après qu'elles aient eu lieu. En contrepartie, on perd une part de la bande passante avec les paquets de contrôle RTS, CTS et ACK. C'est une des raisons pour lesquelles le débit réel en 802.11 est bien inférieur au débit théorique (c'est-à-dire le débit au niveau physique) : le CSMA/CA et le mécanisme RTS/CTS induisent des pertes importantes de débit au niveau de la couche MAC.

Alors pourquoi ne pas simplement utiliser le CSMA/CD ? Il y a deux raisons à cela. D'abord, la plupart des périphériques sans fil sont physiquement incapables d'émettre et de recevoir en même temps : on dit qu'ils sont *Half-Duplex*[1] par nature, un peu comme un talkie-walkie. Par conséquent, ils ne peuvent pas détecter les collisions (contrairement aux équipements Ethernet) et ne peuvent donc pas utiliser le CSMA/CD. La deuxième raison s'explique facilement par l'exemple suivant : mettons trois stations WiFi en ligne de telle sorte que la première soit à portée de signal radio de la seconde, mais pas de la troisième. Dans ce cas, même si toutes les stations sont *Full-Duplex*, les deux stations situées aux extrémités peuvent « parler » à la station du milieu au même instant, sans détecter de collision. La station du milieu aura alors du mal à comprendre quoi que ce soit car elle recevra au même moment des messages provenant de ses deux voisines. Ces collisions diminueront alors considérablement le débit. Pour ces deux raisons, il faut une solution préventive plutôt que curative au problème des collisions : en d'autres termes, on doit éviter que les collisions ne

1. En *Half-Duplex*, on ne peut pas émettre et recevoir en même temps, contrairement au *Full*-Duplex.

surviennent, plutôt que de chercher à les détecter une fois qu'elles ont eu lieu. C'est là tout l'intérêt du DCF.

Dans la pratique, on se rend bien compte que les paquets RTS et CTS ne servent pas à grand-chose quand les paquets de données à émettre sont petits et c'est pourquoi le standard 802.11 autorise les équipements à ne pas émettre de RTS pour les petits paquets. Ce que l'on entend par « petit » est variable : le seuil est souvent fixé par défaut à 1 000 octets, mais certains équipements permettent de le configurer manuellement : le paramètre s'appelle alors en général le RTS *Threshold* (seuil RTS). Il est également possible de désactiver complètement le mécanisme RTS/CTS. Ceci dit, plus le nombre d'équipements et le volume de données échangées augmentent, plus les paquets RTS/CTS s'avèrent importants pour éviter les collisions.

Comme l'Ethernet, le WiFi réagit assez mal lorsque le nombre d'équipements communiquant en même temps est important, car les collisions sont alors beaucoup plus nombreuses. De plus, si une seule station communique à bas débit (à 1 ou 2 Mb/s, par exemple), alors toutes les autres stations sont pénalisées. C'est le cas si une station se trouve loin de l'AP auquel elle est associée. Imaginez-vous dans une salle de réunion, avec des dizaines de personnes cherchant à parler en même temps, dont certaines s'expriment très lentement et vous aurez une image précise des limites du mode DCF.

> Le partage des ondes avec la stratégie DCF est simple et efficace lorsqu'il y a peu d'équipements communiquant en même temps. S'ils sont nombreux, le débit peut chuter considérablement. En outre, si une station communique à bas débit, elle ralentit toutes les autres.

En outre, puisque chaque station doit attendre le silence pour communiquer, la présence d'une interférence continue peut interrompre 100 % du trafic. Ceci peut arriver à proximité d'un équipement industriel, d'un four à micro-ondes en fonctionnement, voire même à cause d'un brouillage volontaire.

Pour finir, le mécanisme CSMA est par nature non déterministe, c'est-à-dire qu'il ne permet pas de garantir le moindre temps de transit puisqu'il repose sur un mécanisme aléatoire. Ceci n'est pas gênant lorsqu'on transmet des données « asynchrones » comme des e-mails par exemple, car la fluidité du transfert n'a pas d'importance. En revanche, si l'on souhaite transférer des données « synchrones » comme de la voix ou de la vidéo, par exemple, la fluidité est essentielle et le CSMA/CA peut devenir insuffisant.

Pour ces trois raisons, le standard 802.11 a défini un autre mode de partage du média de communication : le mode PCF.

3.2.2 Le mode PCF

La deuxième stratégie de partage des ondes radio s'appelle la fonction de coordination par point (*Point Coordination Function*, PCF). Toutes les stations sont reliées (sans fil) à un point d'accès (AP) qui s'occupe de distribuer la parole à chacun. Par nature, cette stratégie n'est donc pas possible en mode Ad Hoc pour lequel les stations sont

connectées directement entre elles sans passer par un AP (voir § 3.3). Puisqu'un AP s'occupe de distribuer la parole, il n'y a plus de collision possible et le temps de latence est donc garanti. En anglais, on dit que ce système est *Contention Free* (CF), c'est-à-dire libre de toute dispute.

Pour reprendre l'analogie de la salle de réunion, cela revient à avoir un organisateur dont le rôle est de coordonner les communications entre les différentes personnes dans la salle. L'AP se tourne successivement vers chacune des stations et lui alloue un « temps de parole » plus ou moins long, grâce à une requête *CF-Poll*[1]. Si la station accepte de prendre la parole, elle doit immédiatement acquiescer avec un paquet CF-ACK. Elle peut alors émettre un ou plusieurs paquets pendant cette période. Si elle n'a toujours rien émis au bout d'un court intervalle appelé le *PCF Inter Frame Space* (PIFS), alors l'AP passe à la station suivante. Les autres stations attendent patiemment.

Le mode PCF permet ainsi de diviser le temps de parole plus équitablement entre les stations et surtout de façon plus fluide et déterministe : ce mode est donc intéressant pour transférer des données synchrones, telles que des communications multimédias.

En contrepartie, une portion importante de la bande passante peut être gâchée si de nombreuses stations n'ont rien à émettre : lorsque la parole leur est donnée, les autres stations attendent, en définitive, pour rien.

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

Pour qu'une station sache exactement quand elle peut parler librement et quand elle doit attendre qu'on lui donne la parole, il faut qu'elle soit parfaitement synchronisée avec l'AP. Cette synchronisation est assurée par des trames « balises » envoyées régulièrement par l'AP (fig. 3.6). Chaque balise indique le début d'une séquence PCF/DCF et indique la durée de la séquence totale ainsi que la durée maximale de la phase PCF. À tout moment pendant la phase PCF, l'AP peut décider de passer à la phase DCF en envoyant un paquet à toutes les stations (broadcast) appelé le *CF-End*.

Un point important : le PIFS est plus court que le DIFS, de sorte que si une station ne connaît pas le mode PCF, elle ne pourra pas prendre la parole pendant la phase PCF, car elle ne détectera jamais de silence assez long. Une station compatible uniquement avec le DCF peut donc se connecter à un AP configuré en mode PCF, mais elle disposera d'une bande passante plus faible que les autres stations car elle ne pourra communiquer que pendant la phase DCF. Bien entendu, si une station compatible avec le PCF se connecte à un AP qui ne gère pas ce mode, elle passera automatiquement au mode DCF.

1. *Poll* signifie « sondage » ou « interrogation ».

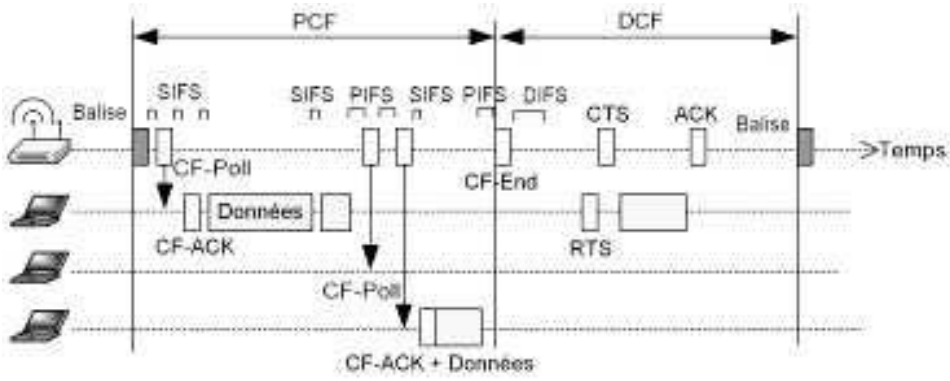


Figure 3.6 — Le fonctionnement du mode PCF.

Dans la pratique, le mode PCF est très peu répandu. Bien qu'il ait été défini dès la première version du standard en 1997, les premiers produits le mettant en œuvre ne sont parus qu'en 2002. En outre, le PCF n'est pas obligatoire, contrairement au DCF et la WiFi Alliance n'inclut malheureusement pas le PCF dans ses tests d'interopérabilité : il est donc possible que deux équipements PCF ne fonctionnent pas correctement ensemble s'ils ne sont pas issus du même constructeur. Bref, pour mieux gérer le trafic multimédia, il vaut mieux utiliser des produits mettant en œuvre le 802.11e.

3.2.3 Les améliorations du 802.11e

Bien que le PCF offre un mécanisme pour garantir un débit fluide et permette ainsi d'améliorer la qualité de service (QoS) pour des applications multimédias, le 802.11e apporte une solution plus complète :

- d'une part, chaque paquet WiFi peut être associé à une classe de trafic (*Traffic Class*, TC, également appelée *Access Category*, AC) particulière. Concrètement, cela signifie qu'un numéro lui sera rajouté, indiquant son niveau de priorité. On peut avoir jusqu'à huit TC et un AP doit en mettre en œuvre au minimum quatre ;
- d'autre part, deux nouvelles fonctions de coordination sont définies. Elles traitent les paquets différemment selon la TC à laquelle ils appartiennent. Ces fonctions sont l'*Enhanced* DCF et l'*Enhanced* PCF (c'est-à-dire « DCF et PCF améliorés »)[1].

1. Dans le standard, ratifié fin 2005, on parle maintenant de EDCA (Enhanced *Distribution Channel Access*) et de HCCA (*Hybrid-Coordination-Function Controlled Channel Access*).

L'EDCF

L'EDCF est très proche du DCF, mais les paquets de haute priorité ont plus de chances d'être émis rapidement que ceux de basse priorité. Souvenez-vous qu'avec la DCF, une station commence par attendre un silence d'une durée minimale appelée le DIFS, puis elle attend pendant une période aléatoire au sein d'une fenêtre de collision (CW). Avec le mode EDCF, le délai DIFS et la fenêtre de collision CW peuvent être réglés pour chaque classe de trafic[1]. On ne parle plus de DIFS mais de *Arbitration Inter Frame Space* (AIFS) dont la durée est supérieure ou égale au DIFS. La classe la plus prioritaire aura un AIFS plus court et une fenêtre de collision plus petite qu'une classe moins prioritaire : ainsi, un paquet prioritaire passera plus souvent devant un paquet moins prioritaire.

SIFS < PIFS < DIFS < AIFS (fonction de la classe de trafic).

En outre, chaque station gère une file d'attente par classe de trafic et applique les mêmes règles probabilistes pour déterminer de quelle file d'attente elle prendra le prochain paquet à émettre. Un paquet commence donc par être placé dans une file d'attente adaptée à sa classe de trafic, puis lorsque son tour est arrivé, il doit gagner successivement deux « batailles » avant d'être transmis : la première contre les paquets des autres files d'attente du même adaptateur (bataille interne) et une seconde contre les paquets des autres stations (bataille externe).

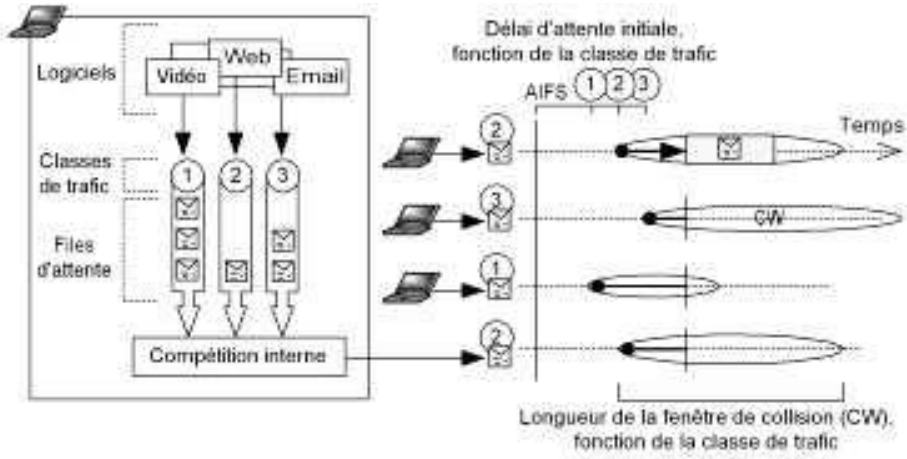


Figure 3.7 — Le mode EDCF : une compétition interne puis externe.

L'EDCF permet également aux stations d'envoyer plusieurs paquets d'affilée. Dans ce cas, on dit que la station profite d'une « opportunité de transmission », notée TXOP. La durée maximale d'une TXOP peut être précisée dans les trames balises de l'AP.

1. Puisque la CW augmente à chaque collision, certains équipements permettent de régler la CW maximale pour chaque classe de trafic.

Pendant une TXOP, la station émet autant de paquets qu'elle le souhaite, les uns après les autres en ne les espaçant que de SIFS. Puisque SIFS est le délai le plus court possible, personne ne peut l'interrompre. Pendant la TXOP, les paquets de la station émettrice n'ont qu'une seule bataille à gagner : la bataille interne.

Si le réseau est composé de plusieurs stations DCF simples et d'autres gérant l'EDCF, alors les stations DCF auront tout simplement une seule classe de trafic, de priorité moyenne. Les stations EDCF pourront fonctionner normalement et leur trafic de haute priorité passera en général avant le trafic des stations DCF.

Ce système est relativement simple à mettre en œuvre et il permet de régler les priorités des flux en fonction des classes de trafic. Malheureusement, puisqu'il repose sur le hasard, il peut arriver que quelques paquets prioritaires soient retardés un peu trop longtemps, par malchance. Inversement, certains paquets peu prioritaires peuvent être émis avec beaucoup de retard s'il y a un trafic régulier et plus prioritaire sur le réseau : c'est ce qu'on appelle la « famine ». Dans la plupart des cas, ce ne sera pas dramatique, mais pour certaines applications, il est préférable d'utiliser l'EPCF.

La WiFi Alliance a défini la certification *Wireless MultiMedia Extensions* (WME), également appelée *WiFi Multimedia* (WMM), pour les produits compatibles avec l'EDCF.

L'EPCF

Cette stratégie de coordination est également appelée la fonction de coordination hybride (*Hybrid Coordination Function*, HCF). Elle étend le principe du PCF en lui rajoutant la gestion des classes de trafic. Le principe de base de l'EPCF est très similaire au PCF : dans une première phase, l'AP contrôle le temps de parole des stations, puis dans une seconde phase, toutes les stations peuvent prendre la parole librement, selon le mode EDCF et ces deux phases alternent indéfiniment. Toutefois, l'EPCF est légèrement plus flexible, car même pendant la deuxième phase, l'AP peut donner la parole à une station. Pour cela, l'AP attend le premier silence d'une longueur de PIFS. Puisque PIFS est inférieur à DIFS et AIFS, l'AP est assuré d'obtenir la parole. En outre, lorsqu'une station obtient la parole, elle dispose d'une TXOP, comme pour l'EPCF et peut donc envoyer plusieurs paquets en série.

Revenons à l'analogie de la salle de la réunion : l'organisateur commence par diriger la réunion, en donnant la parole successivement aux personnes de son choix. En mode PCF, il donnait la parole à tout le monde à tour de rôle (en boucle), mais avec l'EPCF il peut être plus malin et choisir l'ordre qu'il veut, en fonction de paramètres aussi complexes qu'il le souhaite. Ensuite, lorsque la phase « dirigée » est terminée, soit parce qu'elle a durée le temps prévu, soit avant si l'organisateur en a décidé ainsi (comme en mode PCF), on entre dans la phase de discussion libre. Dans cette phase, ceux qui ont des choses importantes à dire ont tendance à prendre la parole plus rapidement et donc à parler plus souvent : c'est l'EDCF. À tout instant, l'organisateur peut interrompre tout le monde et donner la parole à une personne, s'il le souhaite. Chaque fois qu'une personne a la parole, elle peut la garder pendant un temps limité

et émettre plusieurs idées d'affilée. Une fois que cette phase « libre ou presque » est terminée, on revient en phase « dirigée » et ainsi de suite.

Afin de pouvoir donner intelligemment la parole, l'AP peut souhaiter connaître la longueur des files d'attentes de chaque station, pour chaque classe de trafic. Les stations indiquent donc cette information au début de chaque paquet, dans l'en-tête MAC modifié à cet effet par le 802.11e. L'AP peut alors donner la parole aux stations, en prenant en compte, par exemple :

- la priorité de la TC ;
- le type de QoS requis pour cette TC : par exemple, un faible temps de latence, une bande passante importante, un débit régulier pour éviter les à-coups (*jitter*), etc. Ceci peut être configuré dans l'AP ;
- la longueur des files d'attentes pour chaque station ;
- le temps de parole cumulé pour chaque station ;
- et tout autre paramètre.

Lorsque l'AP donne la parole à une station, il ne lui impose pas une file d'attente à utiliser. Ceci permet de déléguer une partie du travail et de responsabilité à chaque station, afin d'alléger le travail de l'AP : son rôle se réduit donc à distribuer correctement le temps de parole entre les stations. Notons que l'AP peut se donner la parole à lui-même, ce qui arrive d'ailleurs très souvent car il doit relayer tout le trafic en provenance et à destination des stations.

Le mode EPCF du 802.11e est le plus flexible mais également le plus complexe : il peut gérer finement la QoS pour chaque classe de trafic.
La WiFi Alliance propose la certification WMM-Scheduled Access pour les produits compatibles avec le mode EPCF du 802.11e. Malheureusement, à ce jour, le WMM-SA n'a été mis en œuvre que dans quelques produits seulement et semble abandonné par l'industrie au profit du WMM.

3.2.4 Le paramétrage et la compatibilité

Résumons : la stratégie la plus répandue est le DCF, qui stipule un partage simple du temps de parole, basé sur le hasard. Le PCF découpe le temps en tranches régulières délimitées par des balises. Chaque tranche de temps est divisée en deux phases : dans la première, l'AP donne la parole successivement à chaque station, à tour de rôle et dans la seconde, les stations peuvent prendre la parole librement, comme avec le DCF. Le 802.11e a rajouté dans chaque paquet un numéro indiquant la classe de trafic à laquelle il appartient. Par ailleurs, il a défini l'EDCF et l'EPCF, deux stratégies similaires au DCF et au PCF, mais prenant en compte la notion de TC.

Pour le DCF ainsi que pour toutes les autres stratégies, le paramètre RTS Threshold peut s'avérer utile pour régler finement les performances de votre réseau. Il permet de fixer la taille des paquets à partir de laquelle il faut demander la parole (requête RTS) avant d'envoyer le paquet. Il peut être intéressant d'augmenter ce paramètre si le nombre de stations susceptibles de communiquer en même temps est faible, ou de

le diminuer dans le cas contraire. Le plus sûr est de mesurer la performance du réseau et de modifier ce paramètre pour trouver la valeur optimale.

Pour le PCF, il faut d'abord s'assurer que tous les équipements soient bien compatibles entre eux s'ils proviennent de constructeurs différents. Ensuite, le principal réglage consiste à fixer la durée de la phase « dirigée » par rapport à celle de la phase « libre ». À moins de travailler sur du vieux matériel, il est recommandé de passer plutôt au 802.11e.

Dans le cas de l'EDCF, le paramétrage est un peu plus complexe, car il faut configurer les paramètres des classes de trafic et la durée maximale d'un temps de parole (TXOP). Heureusement, les AP 802.11e sont fournis avec des paramètres par défaut plutôt satisfaisants. Il n'est pas forcément dramatique que quelques stations ne gèrent pas le 802.11e, car la stratégie EDCF est compatible avec la DCF, qui est gérée par tous les équipements WiFi. Toutefois, les stations en DCF n'auront qu'une seule classe de trafic. Alternativement, il est parfois possible de mettre à jour les équipements pour le 802.11e en installant une version plus récente du *firmware*, que l'on peut souvent télécharger sur le site web du constructeur.

Le paramétrage de l'EPCF est le plus complexe car il faut à la fois configurer les paramètres EDCF et les paramètres propres à l'EPCF. Presque toute la logique de l'EPCF est mise en œuvre dans l'AP : son rôle est de distribuer intelligemment la parole, mais reste à définir ce qu'on entend par « intelligemment ». Dans certains cas, il s'agit simplement de donner la parole successivement à chaque station, comme en PCF. Mais cela peut également être une logique beaucoup plus complexe, prenant en compte la priorité et la politique de QoS des classes de trafic, la longueur de la file d'attente de chaque station, ou encore des statistiques sur le trafic passé. Ceci dépend donc de chaque AP.

Toutes les stratégies sont compatibles entre elles : nous avons déjà vu que le PCF était compatible avec le DCF : simplement, les stations DCF auront un débit plus faible. En outre, contrairement au 802.11 qui n'imposait pas le PCF, le 802.11e impose qu'à la fois l'EDCF et l'EPCF soient mis en œuvre. *Résultat* : la question de l'interopérabilité ne se pose pas vraiment. D'une façon générale, si le réseau est hétérogène, la qualité de service correspondra à la fonction la plus simple.

Notons enfin que le 802.11e a un défaut : rien n'empêche en principe un utilisateur mal intentionné de configurer son poste pour donner une priorité élevée à toutes les données qu'il émet. Pour limiter cela, il faut mettre en place un système capable de détecter et de déconnecter les « tricheurs » (par exemple intégrés aux AP).

3.3 LE RÉSEAU AD HOC OU INFRASTRUCTURE

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

3.3.1 Le mode Infrastructure

Dans les réseaux de type Infrastructure, chaque périphérique est relié au réseau *via* un point d'accès (AP) WiFi. On dit que le périphérique est le « client » et l'AP le « maître ». Un réseau de ce type s'appelle un *Basic Service Set* (BSS, fig. 3.8) et couvre un espace qu'on appelle une « cellule » ou *Basic Service Area* (BSA). Chaque BSS est identifié par un nombre composé de 48 bits : c'est le BSSID. En mode Infrastructure, ce BSSID correspond tout simplement à l'adresse MAC du point d'accès. L'AP sert de relais entre les périphériques, mais il peut aussi servir de relais vers un réseau filaire, par exemple votre réseau d'entreprise.

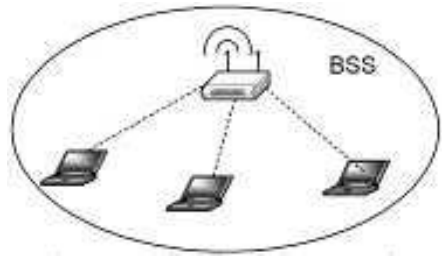


Figure 3.8 — Un réseau Infrastructure composé d'une seule cellule (BSS).

Plusieurs points d'accès peuvent être déployés pour atteindre une plus large couverture WiFi. Ces BSS multiples peuvent être reliés par un système de distribution (*Distribution System*, DS) de façon à former un unique réseau sans fil étendu. Le DS peut être un réseau filaire Ethernet (cas le plus fréquent), un câble de point à point, ou encore une liaison sans fil ! Il est alors possible à un utilisateur de se déplacer dans l'ensemble de la zone de couverture sans souffrir de ralentissement ou d'interruption de sa connexion : en cas de besoin, la liaison bascule automatiquement (c'est le *hand-over*) vers le point d'accès offrant la meilleure connexion. On parle dans ce cas d'*Extented Service Set* (ESS, fig. 3.9) qui couvre naturellement un espace appelé l'*Extended Service Area* (ESA), composé de plusieurs cellules. Chaque ESS est identifié par un nom stocké sur 32 octets maximum qui s'appelle l'ESSID (ou simplement le SSID)[1]. Il faut faire attention à ce que deux ESS distincts dont les cellules se superposent aient toujours des noms (SSID) différents, sinon on observera des problèmes de connexion importants dans les zones de superposition.

3.3.2 Le mode Ad Hoc et les réseaux maillés

Dans les réseaux de type Ad Hoc, chaque périphérique communique directement avec les périphériques situés à sa portée, sans passer par un intermédiaire. Ce mode

1. L'encodage des caractères du SSID n'est malheureusement pas spécifié par le standard. Si le SSID contient des caractères accentués, ils risquent d'être mal affichés sur le poste de l'utilisateur. Avec certains systèmes, le SSID sera même totalement ignoré ou la connexion impossible. Il est donc conseillé de se contenter des caractères ASCII : le SSID peut alors avoir jusqu'à 32 caractères.

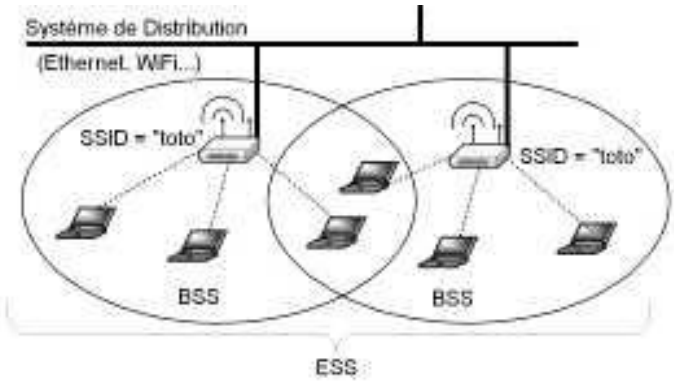


Figure 3.9 — Un réseau Infrastructure comportant plusieurs cellules (ESS).

est pratique pour l'échange de données entre quelques stations en l'absence d'une quelconque infrastructure réseau (aucun point d'accès). Le réseau ainsi constitué s'appelle un *Independent Basic Service Set* (IBSS, fig. 3.10).

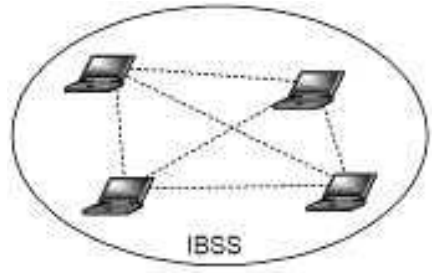


Figure 3.10 — Plusieurs stations reliées directement entre elles en mode Ad Hoc (IBSS).

Malheureusement, le mode Ad Hoc a deux inconvénients majeurs. Premièrement, il peut parfois être assez pénible à configurer. En effet, imaginons quelques personnes qui souhaitent simplement s'échanger des fichiers avec le mode Ad Hoc. Dans ce cas, l'un d'entre eux pourra configurer son adaptateur WiFi en mode Ad Hoc, en précisant le canal WiFi et le SSID à utiliser. Les autres pourront alors s'associer à ce réseau Ad Hoc en le détectant avec leur adaptateur WiFi, ou bien en configurant eux-mêmes leur propre adaptateur WiFi. Ensuite, à moins que l'un d'entre eux n'ait configuré un serveur DHCP[1] sur son ordinateur (ce qui n'est pas fréquent), ils devront se mettre d'accord sur une configuration IP et configurer leur système d'exploitation en conséquence. Ensuite, il leur faudra encore activer le partage de fichier ou démarrer un serveur FTP. Bref, ce n'est pas à la portée de tout le monde. Vous remarquerez sans doute que la configuration du réseau WiFi lui-même n'est pas très compliquée, mais

1. Si vous ne connaissez pas le DHCP, veuillez consulter l'annexe A qui présente les réseaux IP sur *www.livrewifi.com*.

toute la lourdeur provient du fait que les couches réseaux supérieures doivent être paramétrées manuellement car on ne dispose pas des ressources habituellement mises en œuvre sur un réseau d'entreprise : un serveur DHCP, un serveur de fichiers, etc. C'est sans doute la raison principale pour laquelle ce mode est beaucoup moins utilisé que le mode Infrastructure.

> Pour relier plusieurs ordinateurs entre eux en mode Ad Hoc, il faut configurer le réseau au niveau WiFi, mais aussi au niveau IP.

Deuxièmement, ce mode Ad Hoc ne spécifie par comment deux stations peuvent communiquer entre elles par l'intermédiaire d'une troisième : aucun protocole de routage n'est prévu. Autrement dit, le mode Ad Hoc ne permet que de parler avec ses voisins directs, et il ne permet pas, tout seul, la mise en place ce qu'on appelle un « réseau maillé » (en anglais, « *mesh network* »), c'est-à-dire un réseau où les stations peuvent communiquer les unes avec les autres par l'intermédiaire d'autres stations. Pour y parvenir, on doit rajouter au mode Ad Hoc un protocole de routage adapté aux réseaux maillés. Jusqu'à présent, il n'existait pour cela qu'une seule solution : installer sur chaque station un logiciel propriétaire qui se charge du routage (il existe différentes solutions, donc on doit faire attention à installer le même logiciel partout). Ce logiciel commence par établir un dialogue avec toutes les stations voisines, en mode Ad Hoc, puis il met en œuvre un protocole de routage bien adapté aux réseaux maillés, comme *Optimized Link State Routing* (OLSR) ou *Ad hoc On-Demand Distance Vector* (AODV). Le protocole de routage permet d'acheminer chaque paquet vers sa destination, en passant si nécessaire par des stations intermédiaires. On peut ainsi profiter d'un réseau étendu, sans installation de points d'accès, avec un débit toutefois beaucoup plus limité. Malheureusement, le coût de ces logiciels et le fait qu'il s'agisse de solutions propriétaires a limité fortement le déploiement de réseaux maillés jusqu'à présent.

Cette situation est en train de changer : l'IEEE a publié en 2006 une ébauche (*draft* 0.01) du futur standard 802.11s pour les réseaux maillés. On s'achemine actuellement vers la fin du processus de standardisation, le *draft* 3.00 ayant été publié en mars 2009, et étant considéré comme assez stable. Le 802.11s définit le protocole de routage nommé *Hybrid Wireless Mesh Protocol* (HWMP) : il s'agit d'une combinaison du protocole AODV et de techniques de routage reposant sur l'élaboration automatique d'un graphe arborescent entre les stations (un graphe où les boucles sont éliminées). Le 802.11s autorise toutefois l'utilisation d'autres protocoles de routage. Le principal déploiement actuel du 802.11s est sans doute le projet américain *One Laptop Per Child* (OLPC) qui vise à fournir un ordinateur portable à faible coût pour les enfants des pays en voie de développement, à des fins d'éducation : ces ordinateurs peuvent se connecter les uns aux autres en mode Ad Hoc et former un réseau maillé grâce au 802.11s, sans qu'il soit nécessaire d'installer de point d'accès. Le 802.11s peut également être installé dans des points d'accès : ceci permet notamment à des stations connectées entre elles en un réseau maillé de pouvoir se connecter à un réseau filaire (lui-même connecté à Internet, par exemple). Cela permet aussi de relier des points d'accès entre eux par des connexions sans fil, selon une architecture maillée, résistante à l'éventuelle défaillance d'un des points d'accès.

Le 802.11s est déjà disponible sous Linux depuis la version 2.6.26 du noyau (kernel), grâce au projet libre Open80211s, promu par un consortium de constructeurs de matériels 802.11s. Il sera sans doute à terme inclus par défaut dans Windows et Mac : pour l'heure, il faut installer un pilote 802.11s.

3.4 LE PROCESSUS D'ASSOCIATION

3.4.1 Les trames « balises »

En mode *Infrastructure*, chaque point d'accès émet à intervalles réguliers (en général toutes les 100 ms, soit 10 fois par seconde) des trames[1] particulières appelées les trames balises (*beacon frame*). Les balises contiennent des informations concernant le point d'accès, dont en particulier le BSSID, les débits autorisés et éventuellement le SSID.

Le standard reste assez ouvert sur les informations diffusées dans les trames balises, ce qui permet à certains constructeurs de rajouter des informations spécifiques, comme la charge actuelle de l'AP, pour permettre aux équipements sachant interpréter ce paramètre de se connecter à l'AP le moins encombré. Il est fort probable que de nouveaux paramètres seront standardisés régulièrement par l'IEEE.

Un autre rôle important des trames balises est de garantir la synchronisation entre toutes les stations qui lui sont associées. Pour cela, elles contiennent un champ qui indique avec précision le temps écoulé depuis l'initialisation de l'AP. Cette synchronisation est indispensable lorsque l'AP est configuré pour utiliser le mode PCF ou EPCF, comme nous l'avons vu, ou encore lorsque des stations utilisent le mode d'économie d'énergie (voir § 3.6.4).

3.4.2 Détecter les réseaux présents

La diffusion (ou *broadcast*) du SSID dans les trames balises est une option de l'AP. Un équipement WiFi peut donc facilement établir « passivement » la liste des SSID déclarés des réseaux sans fil situés à proximité, sans même avoir à émettre le moindre signal. Sur un ordinateur, l'utilisateur pourra ainsi très simplement sélectionner le SSID de son choix dans une liste.

Il est également possible de faire une recherche active des points d'accès présents : un périphérique peut en effet envoyer des requêtes de sondage (*probe requests*) sur chaque canal qui l'intéresse (en fonction des canaux autorisés dans le pays où l'on se situe), contenant le SSID souhaité et les débits que le périphérique est capable de gérer. Si un point d'accès se situe à proximité et reçoit la requête, il commence par vérifier que le SSID correspond au sien et si c'est le cas il répond avec un paquet (*probe response*) contenant à peu près la même chose que la trame balise

1. Une trame est un paquet de données émis au niveau physique. Un paquet de données d'une couche supérieure (par exemple un paquet IP) peut être découpé et émis dans plusieurs trames physiques distinctes (voir § 2.5).

(fig. 3.11). Ce mécanisme est plus fiable que la méthode passive car on est assuré que la communication peut bel et bien avoir lieu dans les deux sens. En contrepartie, des requêtes de sondage trop fréquentes peuvent baisser légèrement la performance d'un réseau sans fil.

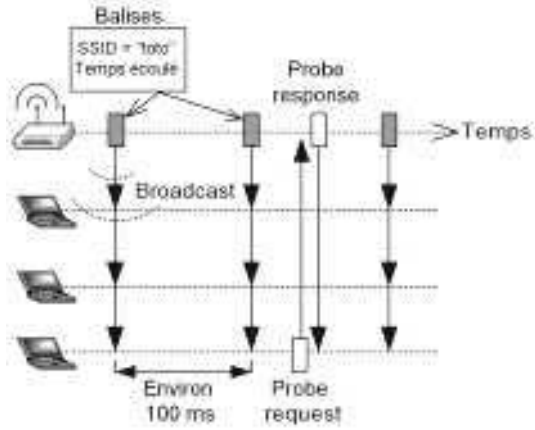


Figure 3.11 — Les balises et les requêtes de sondage.

3.4.3 L'authentification

Pour pouvoir communiquer sur un réseau sans fil de type *Infrastructure*, une station doit d'abord s'identifier auprès d'un AP avant d'y être associée.

Pour s'identifier, la station envoie une requête d'« authentification » à un AP, avec le SSID voulu. Si le réseau n'est pas sécurisé par une clé WEP, aucune information d'identification n'est requise et la réponse est toujours positive (pourvu que le SSID soit le bon, bien entendu). On parle d'authentification « ouverte »[1] (*Open Authentication*).

En revanche, si le réseau est sécurisé par une clé WEP, l'AP renvoie dans sa réponse un « défi » (ou *challenge*) : il s'agit d'un nombre aléatoire de 128 bits que la station doit crypter en utilisant sa clé WEP (*Wired Equivalent Privacy*)[2]. Le résultat crypté est alors envoyé à l'AP dans une nouvelle requête d'authentification. Celle-ci peut alors vérifier que le résultat est le bon en réalisant elle-même le cryptage avec sa propre clé WEP : si elle trouve le même résultat, elle sait que la station possède bien la bonne clé et dans ce cas elle renvoie une réponse positive.

Le standard 802.11 semble avoir tout prévu... Malheureusement, ce procédé possède de graves défauts : tout d'abord, il permet à l'AP d'identifier que la station est légitime, mais l'inverse n'est pas vrai. Au cours de l'authentification, rien ne garantit

1. Vous verrez parfois des adaptateurs proposant le mode « Ouvrir » : erreur de traduction bien sûr !
2. Nous aborderons rapidement le WEP au § 3.5.3 et nous le détaillerons au chapitre 7.

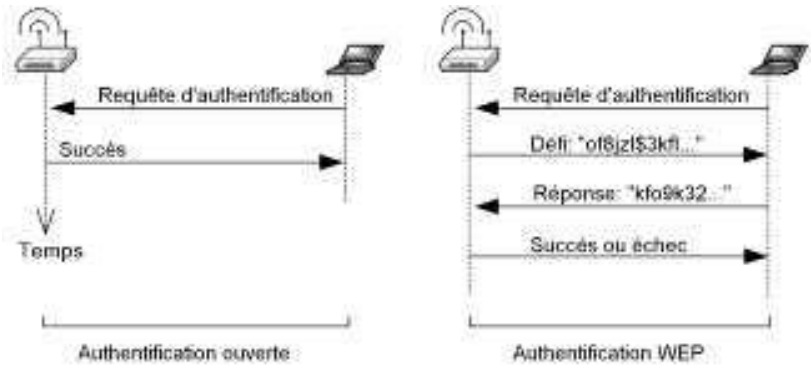


Figure 3.12 — Authentification ouverte et authentification WEP.

à la station qu'elle a bien affaire à un AP du réseau auquel elle souhaite s'associer. En outre, une fois l'authentification terminée, on se retrouve plus ou moins au point de départ : l'AP sait que la station dont l'adresse MAC est « x » est légitime, c'est tout. Or, une adresse MAC peut facilement être imitée. Il suffit donc à un pirate de « sniffer » le réseau sans fil, d'attendre qu'un utilisateur légitime s'authentifie, puis de noter son adresse MAC et de configurer son adaptateur WiFi pour qu'il utilise cette adresse, ce que permettent certains adaptateurs.

Imaginez que vous receviez un appel téléphonique : votre interlocuteur vous salue, vous lui demandez de s'identifier, il vous répond en vous fournissant bien la preuve de son identité, puis il raccroche avant de vous avoir dit ce qu'il avait à vous dire. Quelques minutes plus tard, vous recevez un nouvel appel. La voix est semblable, mais comment être sûr qu'il s'agisse bien de la même personne ? Lors du premier appel, il aurait fallu que vous conveniez d'un « mot de passe du jour », à prononcer au début de chaque nouvel appel pour éviter que votre interlocuteur ne soit obligé de fournir systématiquement toutes les preuves de son identité : on voit que le premier appel n'a pas servi à grand-chose.

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

En deux mots, l'authentification 802.11 n'apporte rien. Pire, elle fournit à un pirate un exemple de message en clair et sa version codée (le défi et la réponse au défi). C'est un indice de plus pour trouver la clé WEP !

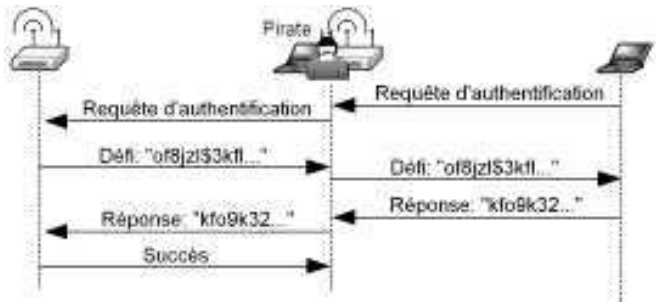


Figure 3.13 — Attaque de type *Man in the Middle* contre l'authentification WEP.

Bref, malgré le fait que l'authentification WEP soit spécifiée par le standard 802.11, elle a été bannie des spécifications WiFi définies par la WiFi Alliance[1]. Rares sont les produits WiFi qui la mettent en œuvre. C'est l'un des rares exemples où le WiFi n'est pas tout à fait fidèle au 802.11. Dans un produit WiFi, il n'y a qu'un seul type d'authentification : l'authentification ouverte.

> L'authentification WEP n'apporte aucune sécurité. Nous verrons comment mieux authentifier les utilisateurs au chapitre 8.

3.4.4 L'association

Lorsque la station a bien été identifiée et que l'AP a renvoyé une réponse d'authentification positive, la station peut alors s'associer à l'AP pour avoir accès aux services du réseau. Pour cela, elle doit envoyer une requête d'association à l'AP. Cette requête contient entre autres la liste des débits que la station est capable de gérer. L'AP alloue un identifiant unique à la station (l'identifiant d'association), elle enregistre les informations de la requête dans sa table des associations (en mémoire), enfin elle renvoie une réponse d'association pour confirmer que l'association a bien eu lieu. À partir de ce moment, la station fait « officiellement » partie du réseau : tout paquet envoyé par cette station est relayé par l'AP.

3.4.5 La réassociation

Malgré son association avec un AP donné, la station vérifie régulièrement (passivement ou activement) la présence d'autres AP ayant le même SSID. Ainsi, lorsqu'un AP s'avère plus intéressant (plus proche ou plus disponible), la station envoie d'abord une requête de « désassociation » auprès de l'AP actuel suivie d'une requête de « réassociation » auprès du nouvel AP. La requête de réassociation indique entre autres l'identité de l'AP précédent. Ceci permet aux deux AP de se mettre en relation

1. Attention, seule l'authentification WEP a été éliminée. Le cryptage WEP peut être utilisé par la suite, une fois la station associée. Dans ce cas, il y aura une authentification implicite et bilatérale puisque seuls les paquets cryptés avec la même clé WEP seront compris par la station et par l'AP.

au travers du système de distribution (DS) pour se transmettre des informations concernant la station et pour distribuer d'éventuels paquets en attente pour la station. Tout ce processus de réassociation se déroule automatiquement, de façon complètement transparente pour les couches réseaux supérieures et pour l'utilisateur : on peut ainsi changer de cellule tout en poursuivant un téléchargement, par exemple.

3.4.6 Et en mode Ad Hoc ?

Contrairement au mode Infrastructure dans lequel un AP central peut synchroniser toutes les stations par l'envoi de trames balises à intervalles réguliers, il n'y a pas d'équipement central en mode Ad Hoc. Comment ce problème est-il résolu ? Très simplement : lorsqu'une station est configurée en mode Ad Hoc, elle attend un certain temps et si elle ne détecte pas de balise, elle l'émet elle-même, à intervalles réguliers. Si d'autres stations rejoignent le réseau Ad Hoc, chaque balise peut être envoyée par n'importe laquelle des stations. En effet, nous avons vu que chaque balise contient le délai précis avant l'émission de la balise suivante. Chaque station attend donc ce délai plus un petit délai aléatoire, comme en DCF et si aucune autre station ne l'a déjà fait, elle envoie la balise. Le hasard désigne donc la station qui émettra la balise, ce qui répartit naturellement cette tâche entre toutes les stations.

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

3.5 LES MÉCANISMES DE SÉCURITÉ

Voici un bref aperçu des solutions de sécurité prévues par le 802.11. Nous approfondirons la sécurité au cours des chapitres 6 à 10.

3.5.1 Masquer le SSID

Puisque toute requête d'authentification doit contenir le bon SSID, on voit qu'un premier niveau de sécurité pour un réseau WiFi consiste à simplement configurer les points d'accès pour qu'ils ne diffusent pas leur SSID. Si quelqu'un ne connaît pas le SSID du réseau, il ne parviendra pas à s'y associer.

Toutefois, cette sécurité est assez faible car il suffit de « sniffer » les paquets de sondage envoyés par les stations « légitimes » du réseau pour pouvoir lire, « en clair » (c'est-à-dire sans cryptage) le SSID du réseau. Il existe des outils très simples disponibles gratuitement pour faire cela. En outre, chaque utilisateur devra saisir à la main (à la première connexion) le SSID, ce qui est pénible et source d'erreurs.

3.5.2 Filtrage par adresse MAC

Bien que cela ne soit pas officiellement dans la norme 802.11, rien n'empêche à un AP de vérifier si l'adresse MAC de la station qui cherche à s'authentifier se trouve bien dans une liste d'adresses MAC autorisées. En effet, l'adresse MAC d'une station est présente dans tous les paquets qu'elle émet, et donc en particulier dans la requête d'authentification. On pourra, par exemple, n'autoriser que les adresses MAC des machines de l'entreprise. Ce type d'authentification peut être employé en complément d'un autre type d'authentification (WEP, WPA, WPA2...).

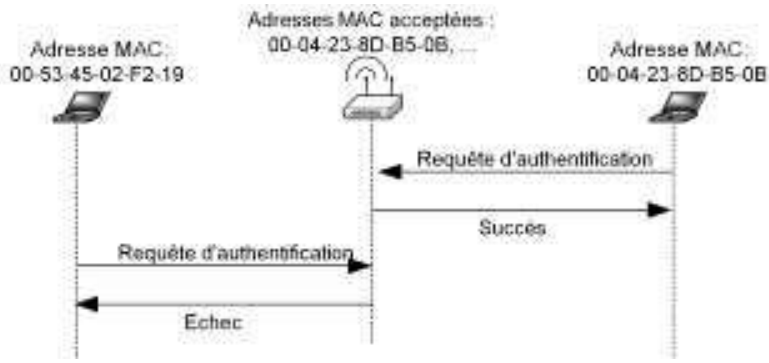


Figure 3.14 — Authentification par adresse MAC.

De nombreux AP du marché gèrent le filtrage par adresse MAC en stockant la liste directement dans l'AP. On peut en général modifier cette liste au travers d'une interface web intuitive.

Malheureusement, il n'est pas très difficile pour un pirate de modifier l'adresse MAC de sa carte WiFi pour se faire passer pour l'un des périphériques autorisés : cela s'appelle le *MAC Spoofing*. Par ailleurs, si le nombre de machines autorisées est important ou change souvent, cette méthode devient assez lourde à gérer. Dans la pratique, le filtrage par adresse MAC offre peu de sécurité et est rapidement lourd à gérer.

3.5.3 Le WEP

La couche MAC du 802.11 offre un mécanisme optionnel de chiffrement des données (cryptage) qui s'appelle le *Wired Equivalent Privacy* (WEP). Tous les périphériques et tous les AP du réseau doivent être configurés avec une même clé secrète de 40 ou 104 bits, qui permet de chiffrer les communications. Le cryptage WEP est suffisamment simple pour être réalisé très rapidement, de sorte qu'il ne pénalise pas (ou peu) le débit.

Il a toutefois plusieurs inconvénients : d'abord, il suppose qu'une même clé soit configurée sur tous les équipements du réseau (AP et périphériques). Cette clé étant connue de tous les utilisateurs du réseau, le risque de « fuite » est plus important car il suffit d'une indiscrétion d'un seul employé pour compromettre toute la sécurité du

réseau. En outre, si la clé est compromise, il faudra la changer sur tous les périphériques et tous les AP, ce qui est très loin d'être pratique. Pour finir, malgré son nom qui signifie littéralement « sécurité équivalente à un réseau filaire », le cryptage WEP a été « cassé » par des chercheurs qui y ont trouvé plusieurs failles. Il existe même des logiciels gratuits pour déchiffrer toutes les communications WEP, ce qui rend ce mécanisme caduc !

> Le cryptage WEP n'offre pas une sécurité suffisante pour un réseau d'entreprise : des logiciels gratuits permettent de le casser.

3.5.4 Le 802.11i et le WPA

Très critiqué pour les failles de sécurité du 802.11, l'IEEE a décidé de réagir en lançant un nouveau groupe de travail : le 802.11i. En 2002, la WiFi Alliance trouvait que le 802.11i tardait à arriver et décida donc de publier une version « légère » du 802.11i, nommée le *Wireless Protected Access* (WPA). Il existe deux variantes : le WPA Entreprise et le WPA Personal. Le WPA Entreprise repose sur le 802.1x et sur un serveur RADIUS et il permet d'assurer une authentification très sécurisée, suivie d'un cryptage robuste des communications : le TKIP. Il est également beaucoup plus souple[1] que le WEP et peut être mis en œuvre dans des grands réseaux d'entreprises.

Le WPA Personal repose sur le simple partage d'une clé secrète sur tous les équipements du réseau, et les échanges sont cryptés par TKIP. Il convient aux petits réseaux.

Le 802.11i a fini par être ratifié en juin 2004. Il complète le WPA avec une méthode de cryptage plus puissante encore : l'AES. La WiFi Alliance a défini la certification WPA2 pour les produits compatibles avec le 802.11i « complet » (avec AES).

> Pour avoir un bon niveau de sécurité, il faut mettre en place la solution WPA, ou mieux, le WPA2. À part pour les très petits réseaux, il est alors nécessaire d'installer et configurer un serveur RADIUS.

Le WPA et le WPA2 Entreprise sont les solutions les plus sûres pour protéger un réseau WiFi au niveau de la couche MAC. Leur principal inconvénient réside dans le fait qu'il est nécessaire de mettre en place un serveur RADIUS, ce qui peut sembler contraignant pour un particulier ou une petite entreprise. Le WPA Personal est donc la solution à privilégier pour un petit réseau sans fil, constitué d'un AP et de quelques stations. Nous reviendrons sur ces solutions dans les chapitres 8 à 10.

1. Le terme anglais *scalable* serait ici plus adapté : il signifie que l'augmentation de la taille du système et du nombre d'utilisateurs, c'est-à-dire la « montée en charge », se fera sans heurts. On pourrait le traduire par « rééchelonnable ».

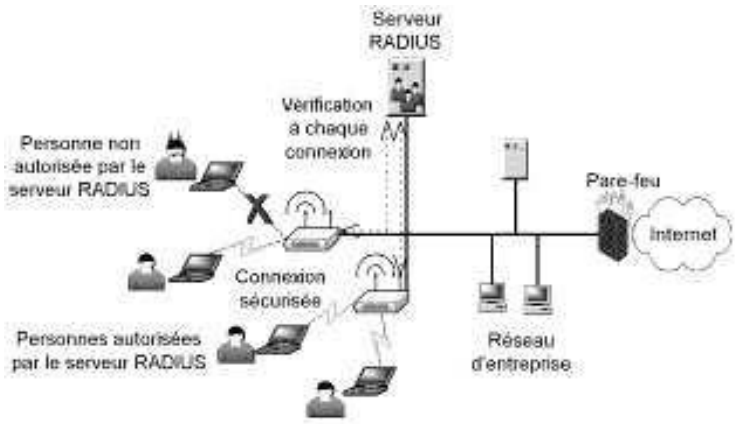


Figure 3.15 — La sécurité WPA ou WPA2 Entreprise avec serveur RADIUS.

3.6 LES AUTRES FONCTIONS MAC

3.6.1 Le contrôle d'erreur

Contrairement à l'Ethernet qui ne s'occupe pas du contrôle d'erreur et laisse les couches supérieures s'en occuper (la couche TCP, en particulier), la couche MAC du 802.11 calcule, pour chaque paquet envoyé, un code de *Contrôle de Redondance Cyclique* (CRC) de 32 bits. Ce code est calculé à partir de l'ensemble des bits du paquet à envoyer et il est rajouté à celui-ci. Ainsi, en recevant un paquet, il suffit d'effectuer le même calcul que l'émetteur (ce qui est très simple et rapide) pour obtenir le CRC du paquet, puis de comparer ce résultat au CRC envoyé par l'émetteur : s'ils sont différents, alors on sait qu'il y a eu une erreur dans la transmission. S'ils sont identiques, il est très probable que le paquet ait été transmis correctement.

Ce mécanisme fait du 802.11 un protocole assez sûr : en cas d'interférences, les paquets erronés seront simplement éliminés. Ainsi, les paquets reçus et validés peuvent être considérés comme très fiables (sauf attaque de pirate, comme nous le verrons). En outre, rien n'empêche d'utiliser au-dessus du WiFi des protocoles de couches supérieures qui fassent eux-mêmes des contrôles similaires.

3.6.2 La fragmentation

Le pourcentage moyen de bits erronés s'appelle le *Bit Error Rate* (BER). Le pourcentage moyen de trames erronées s'appelle le *Frame Error Rate* (FER). Il existe une relation directe entre ces deux valeurs, pour une taille de trame donnée (exprimée en bits) :

$$FER = 1 - (1 - BER)^{taille}$$

Par exemple, si les interférences sont telles qu'en moyenne un bit sur 10 000 est corrompu (BER = 0,01 %, ce qui peut paraître faible au premier abord), alors on peut calculer le FER pour différentes tailles de trames :

- près de 70 % des trames de 1 500 octets (12 000 bits) seront perdues ;
- environ 33 % des trames de 500 octets seront perdues ;
- moins de 8 % des trames de 100 octets seront perdues.

Bref : plus les paquets échangés sont gros, plus il y a de chances pour qu'ils contiennent des erreurs. Si l'environnement radio est de mauvaise qualité, on voit qu'il est très avantageux de découper les gros paquets en plusieurs fragments pour ne pas perdre trop de bande passante avec des paquets corrompus.

La couche MAC du 802.11 fournit un mécanisme de fragmentation des paquets qui peut être très avantageux dans un environnement électromagnétique bruyant. De nombreux adaptateurs WiFi peuvent être configurés pour fixer une taille limite à partir de laquelle un paquet doit être fragmenté. L'émetteur fragmente alors tous les paquets d'une taille supérieure à cette limite et le récepteur s'occupe de rassembler les fragments pour reformer un paquet complet. Ainsi, ce mécanisme est complètement transparent pour les couches réseaux supérieures.

> Dans un environnement électromagnétique bruyant, il peut être intéressant de baisser la taille à partir de laquelle les paquets sont fragmentés.

Chaque fragment est traité normalement, avec son propre code CRC, son en-tête MAC, l'échange éventuel de paquets RTS/CTS, l'envoi d'un paquet ACK lorsque le paquet a bien été reçu, etc. Ainsi, il ne faut pas trop fragmenter les paquets, car cela peut rajouter un surplus de trafic non négligeable et diminuer la bande passante disponible. En outre, en multipliant les paquets, le risque de collision augmente.

Dans un environnement bruyant ou chargé, il est souvent intéressant de modifier ce paramètre manuellement tout en observant (avec un analyseur de réseau sans fil) la quantité de collisions et de paquets rejetés, ou simplement le débit moyen d'un téléchargement : le résultat peut être spectaculaire !

Avant fragmentation, le paquet s'appelle le MAC *Service Data Unit* (MSDU). Le fragment accompagné de son en-tête MAC et de son code CRC s'appelle un MAC *Protocol Data Unit* (MPDU).

Pour finir, notons que pour des raisons d'optimisation, le standard 802.11 interdit à certaines trames d'être fragmentées : c'est le cas des trames balises ainsi que de tout le trafic broadcast et multicast.

3.6.3 L'acheminement des paquets et le WDS

Afin de permettre une gestion aisée des paquets et leur bon acheminement, deux bits sont définis dans l'en-tête de chaque paquet WiFi : le bit *toDS* et le bit *fromDS*. Le premier indique si le paquet s'adresse ou non au système de distribution (c'est-à-dire à un AP) : 1 = oui, 0 = non. Le second précise si le paquet provient du système de distribution ou non. Le tableau suivant présente les quatre possibilités et leur signification.

toDS	fromDS	Mode	Cas de figure
0	0	Ad Hoc	Un paquet envoyé directement d'une station à une autre.
1	0	Infrastructure	Un paquet envoyé par une station vers un AP pour être relayé vers une autre station.
0	1	Infrastructure	Un paquet relayé par un AP vers la station de destination.
1	1	Infrastructure	Un paquet relayé par un AP vers un autre AP pour acheminer le paquet à destination (WDS).

Le dernier cas de figure s'appelle le *Wireless Distribution System* (WDS). Il offre la possibilité à un AP de relayer un paquet non pas directement à la station de destination, mais plutôt à un autre AP, à travers les airs ! Ceci permet d'étendre la couverture du réseau sans fil avec des AP qui ne sont pas connectés au réseau filaire.

Pour permettre l'acheminement d'un paquet à destination, plusieurs adresses sont nécessaires. Dans l'en-tête de tous les paquets WiFi, quatre adresses MAC sont présentes :

- la première adresse représente toujours l'adresse de la prochaine étape du paquet. Par exemple, lorsqu'une station émet un paquet en mode Infrastructure, la première adresse est l'adresse MAC de l'AP (c'est-à-dire le BSSID de la cellule) ;
- la seconde adresse est l'adresse de l'émetteur du paquet. Par exemple, lorsqu'une station émet un paquet, il s'agit de son adresse MAC ;
- la troisième adresse dépend du contexte : en mode Ad Hoc, il s'agit du BSSID de la cellule. En mode Infrastructure, si le paquet est adressé au système de distribution (toDS = 1) alors il s'agit de l'adresse MAC de la station de destination du paquet. Enfin, si le paquet est relayé d'un AP vers une station, cette adresse représente l'adresse MAC de la station source (à l'origine du paquet) ;
- la quatrième et dernière adresse n'est utilisée qu'en mode WDS : il s'agit alors de l'adresse MAC de la station source du paquet.

Voici un tableau récapitulatif :

toDS	fromDS	1re adr.	2e adr.	3e adr.	4e adr.
0	0	Dest.	Source	BSSID	0
1	0	AP	Source	Dest.	0
0	1	Dest.	AP	Source	0
1	1	AP suivant	AP	Dest.	Source

Malheureusement, le standard 802.11 est assez vague sur le mode de distribution WDS et les produits ont tardé à sortir : les premiers produits WDS (à prix raisonnable) sont parus début 2003 et ils sont souvent incompatibles entre eux.

Par ailleurs, un problème important du WDS est le fait que les produits utilisent en général le même canal radio pour recevoir et pour relayer les paquets. Ainsi, la bande passante est divisée par deux à chaque relais. Toutefois, certains produits, assez chers malheureusement, utilisent deux circuits radio configurés sur deux canaux différents, afin d'éviter ce problème : l'un est utilisé pour la fonction d'AP, l'autre pour la fonction de relais.

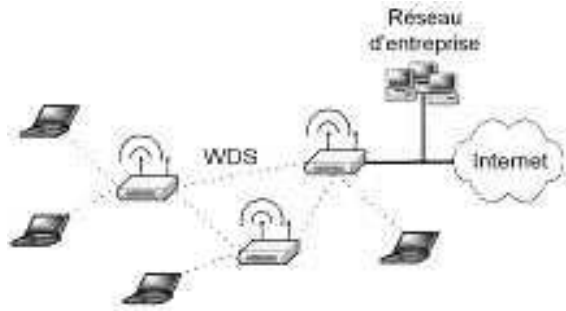


Figure 3.16 — Le Wireless Distribution System (WDS).

Les produits diffèrent en particulier dans leur gestion du « routage » entre les relais : certains n'autorisent qu'un seul relais, d'autre plusieurs. Lorsqu'il y a plusieurs relais possibles, lequel choisir ? On pourrait décider qu'un des relais doit être utilisé en priorité et les autres ne sont là qu'en cas de problème. Ou bien on pourrait choisir d'utiliser tous les relais en boucle, les uns après les autres. Chaque constructeur choisit sa solution.

3.6.4 L'économie d'énergie

La consommation électrique

Les communications radio peuvent consommer beaucoup d'énergie, ce qui est gênant pour des périphériques sans fil dont l'autonomie électrique doit être aussi longue que possible. L'ordre de grandeur n'est pas du tout négligeable : selon le débit des communications et le type de périphérique considéré, les communications WiFi peuvent diminuer l'autonomie du périphérique de plus de 80 % ! Un ordinateur portable ayant habituellement, par exemple, trois heures d'autonomie, n'aura qu'une à deux heures d'autonomie lorsque la connexion WiFi sera très active. De ce point de vue, d'autres technologies sans fil telles que le Bluetooth et le ZigBee sont bien moins « gourmandes » que le WiFi.

Pour définir une stratégie d'économie d'énergie, il faut d'abord savoir à quel moment cette énergie est consommée par un adaptateur WiFi :

- il en consomme le plus lorsqu'il envoie des données ;
- il en consomme un peu moins en recevant des données ;
- lorsqu'il écoute les ondes radio sans rien recevoir, il consomme presque autant que lorsqu'il reçoit un paquet ;
- il ne consomme presque rien lorsqu'il est en sommeil ;
- il ne consomme rien lorsqu'il est éteint.

Pour diminuer la consommation électrique lors de l'émission d'un paquet, une stratégie consiste à diminuer la puissance d'émission. Certains adaptateurs WiFi permettent de régler ce paramètre. Toutefois, cela diminue également la portée du signal, ce qui peut entraîner des problèmes d'émission. Notons que cela n'impacte pas la réception, qui ne dépend bien sûr pas de la puissance d'émission. Pour compenser la diminution de puissance d'émission, on peut installer une antenne directionnelle et la pointer dans la bonne direction. Ceci n'est toutefois pas pratique dans un contexte de mobilité, or c'est là que l'on a besoin d'économiser l'énergie.

Le mode d'économie d'énergie

Dans la pratique, un adaptateur WiFi passe le plus clair de son temps à attendre qu'on lui envoie des paquets. C'est là que l'essentiel de l'énergie est dépensé. Par défaut, les équipements WiFi se trouvent en général dans ce mode de disponibilité continue (*Continuously Available Mode* ou CAM). Une autre stratégie consiste donc à essayer de mettre l'adaptateur WiFi en sommeil aussi souvent que possible. Le 802.11 définit, dans la couche MAC, un mode d'économie d'énergie (*Power Save Polling Mode* ou PSPM, souvent noté PSM) dont c'est précisément le but : mettre l'adaptateur en sommeil dès que possible.

Une station WiFi configurée en mode d'économie d'énergie n'active son interface radio que de façon intermittente (fig. 3.17). Entre chaque envoi et réception de paquets, l'interface radio est simplement éteinte pendant quelques instants. Les paquets devant être envoyés sont placés dans une file d'attente et ne sont émis qu'au « réveil » suivant, de façon groupée. Dans le dernier paquet envoyé à l'AP, la station signale qu'elle va se remettre en mode d'économie d'énergie. L'AP sait alors que tout paquet adressé à cette station devra être mis dans une file d'attente jusqu'à son réveil. À intervalles réguliers, au sein des trames balises, l'AP envoie la liste des stations (plus exactement la liste de leurs identifiants d'association) pour lesquels il possède des paquets en attente. Ce paramètre s'appelle le *Traffic Indication Map* (TIM). De cette façon, au moment d'un réveil, la station n'a pas à émettre de requête pour savoir s'il y a des paquets en attente pour elle : il lui suffit d'attendre de recevoir la liste des stations concernées et de voir si elle en fait partie. Si c'est le cas, elle demande à l'AP de lui envoyer les paquets qui lui sont dus, en lui envoyant une requête *Power Save Poll* (PS-Poll). Sinon, elle se « rendort » immédiatement.

Le trafic broadcast et multicast que l'AP doit émettre est conservé dans une file d'attente et envoyé uniquement à certains moments précis : les stations peuvent ainsi

se réveiller au bon moment pour le recevoir. Pour cela, toutes les quelques balises, l'AP envoie un TIM spécial appelé le *Delivery TIM* (DTIM), qui indique une durée pendant laquelle le trafic broadcast et multicast sera envoyé. L'un des réglages de l'économie d'énergie consiste donc à préciser la durée de la fenêtre de broadcast et la fréquence des DTIM (par exemple, une balise sur cinq).

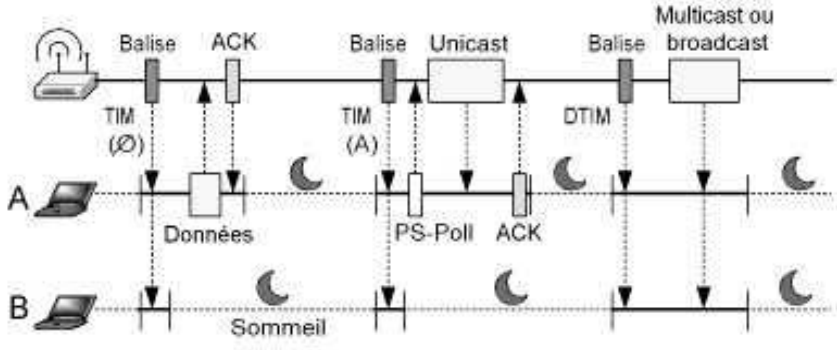


Figure 3.17 — L'économie d'énergie en mode Infrastructure.

En mode Ad Hoc

Pour les communications Ad Hoc, le mécanisme est légèrement différent, mais le principe est le même : si une station est en mode d'économie d'énergie, elle se réveille à intervalles réguliers, au moment de l'émission des balises et elle écoute pendant un bref instant avant de se rendormir (fig. 3.18). Les stations sont synchronisées et toutes celles qui sont en mode d'économie d'énergie se réveillent en même temps. Pour clarifier un peu notre exemple, nous parlerons de « jour » et de « nuit ».

Lorsqu'une station A veut envoyer un paquet de données à une station B qui est en mode d'économie d'énergie, elle doit attendre le « jour » pour s'assurer que la station B soit bien réveillée. Au lieu d'envoyer directement les données, la station A envoie un petit paquet de gestion appelé « l'Annonce TIM » (ATIM). Il signifie à peu près « j'ai des données pour toi ». La station B doit alors immédiatement répondre par un paquet ACK classique. Ensuite, les deux stations attendent la « nuit », mais contrairement à son habitude, la station B ne s'endort pas. Les deux stations peuvent ensuite communiquer normalement pendant toute la « nuit ». À la fin du « jour » suivant, si aucune station n'a de données à envoyer à la station B, celle-ci peut enfin se rendormir.

Économie d'énergie et QoS

Malheureusement, bien que ce mécanisme permette une importante économie d'énergie et donc une plus grande autonomie (très variable selon le type du périphérique et le débit), il peut perturber légèrement la communication WiFi et empêcher tout politique de QoS pour la station qui l'utilise.

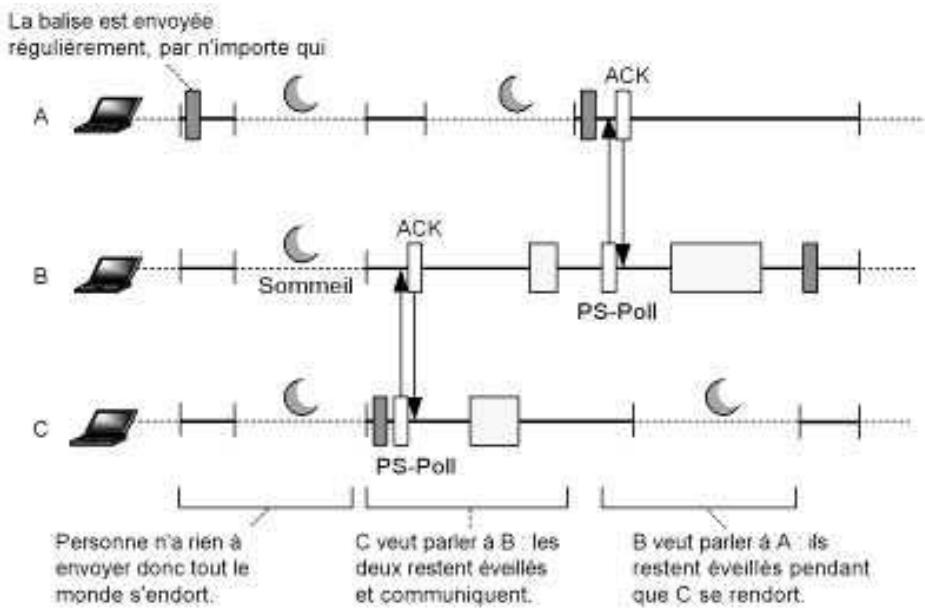


Figure 3.18 — L'économie d'énergie en mode Ad Hoc.

L'économie d'énergie peut être très appréciable pour avoir une autonomie plus importante, mais elle diminue la qualité de la communication : le débit est plus faible et moins fluide.

3.6.5 Le WMM-PS

Pour limiter cet effet négatif de l'économie d'énergie sur la qualité de service, la WiFi Alliance a défini le « WMM-*Power Save* » (ou WMM-PS). Il s'agit d'un ensemble de mesures techniques définies dans le standard 802.11e, et qui ont pour objectif d'optimiser l'économie d'énergie, notamment pour les terminaux mobiles :

- des optimisations du protocole d'économie d'énergie permettent de réduire le temps moyen qu'une station passe « éveillée » ;
- en outre, le WMM-PS permet aux concepteurs de logiciels d'indiquer la priorité du trafic qu'ils gèrent : l'algorithme d'économie d'énergie s'adapte alors automatiquement en fonction de cette priorité. Par exemple, si une station n'a que du trafic peu prioritaire à émettre, elle restera « endormie » plus longtemps, et économisera davantage d'énergie.

3.7 LES PAQUETS WIFI

3.7.1 La structure des paquets

Connaître la structure exacte des paquets WiFi n'est pas réellement utile dans la vie quotidienne, mais en avoir un bref aperçu peut vous aider à mieux comprendre les différentes fonctions de la couche MAC du 802.11 que nous avons abordées dans ce chapitre. Voici donc à quoi ressemble un paquet WiFi, au niveau de la couche MAC ; sous chaque champ est indiquée sa taille :

FC	D/ID	Adr. 1	Adr. 2	Adr. 3	SC	Adr. 4
2	2	6	6	6	2	6
Données						**FCS**
De 0 à 2 304 octets (+8 pour le WEP, ou +20 pour le TKIP, ou +16 pour l'AES)						4

- FC signifie *Frame Control* (contrôle de trame). Ce champ contient lui-même plusieurs autres champs, comme nous le verrons ci-dessous ;
- le deuxième champ représente le temps que prendra l'émission du paquet. Seule exception : pour les paquets PS-Poll, il indique l'identifiant d'association de la station ;
- on retrouve les quatre adresses MAC dont nous avons parlé précédemment au § 3.6.3. Les paquets de contrôle (RTS, CTS...) ne contiennent qu'une ou deux adresses et les paquets de gestion (balises, association...) en contiennent trois (voir § 3.7.2) ;
- SC signifie *Sequence Control* (contrôle de séquence). Ce champ est découpé en deux parties : la première, de 4 bits, est le numéro de séquence du fragment en cours. Lorsqu'un MSDU est fragmenté en plusieurs MPDU, chaque MPDU est numéroté, de sorte que le récepteur puisse reconstituer le paquet. En cas de réémission, le même numéro de fragment est bien sûr réutilisé. La deuxième partie du champ SC, de 12 bits, est le numéro de séquence du MSDU : il est incrémenté pour chaque nouveau MSDU envoyé. Ce champ est absent dans les paquets de contrôle (RTS, CTS, ACK...) ;
- FCS signifie *Frame Check Sequence* (séquence de vérification de la trame). Il s'agit du CRC permettant au récepteur de s'assurer qu'aucune erreur de transmission n'a eu lieu.

Voici le détail du champ FC :

Version		Type		Sous-type			
2 bits		2 bits		4 bits			
toDS	**fromDS**	**Frag**	**Retry**	**Sleep**	**More**	**WEP**	**Order**
1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

- Le premier champ est la version du 802.11 utilisée : pour l'instant, il s'agit toujours de 0.
- Le second indique le type du paquet. Il en existe trois : paquet de gestion (association, authentification...), paquet de contrôle (RTS, CTS, ACK, CF-End...) ou paquet de données (données simples, données + CF-Poll...).
- Le troisième précise le sous-type du paquet : association, RTS, données simples, etc. La liste des types et sous-types est donnée ci-dessous.
- Nous avons déjà parlé du toDS et du fromDS dans la section 3.6.3 : ils servent à indiquer si le paquet s'adresse au système de distribution (toDS) et s'il en provient (fromDS).
- Le champ Frag indique s'il reste encore des fragments après ce paquet.
- Le champ Retry (c'est-à-dire « nouvel essai ») indique que ce paquet est une nouvelle tentative d'émission d'un paquet déjà envoyé précédemment, mais qui n'a pas reçu d'ACK en réponse.
- Le champ Sleep (c'est-à-dire « sommeil ») indique si la station sera en mode d'économie d'énergie (PSM) ou non, après ce paquet.
- Le champ More (c'est-à-dire « plus ») est utilisé par un AP lorsqu'il communique avec une station en mode PSM et qu'il souhaite la prévenir que d'autres paquets seront envoyés après celui-ci. Ceci permet d'éviter que la station ne s'endorme trop tôt et permet également de lui indiquer quand elle peut se rendormir.
- Le champ WEP indique si ce paquet est crypté avec WEP ou non.
- Le champ Order indique que l'émetteur souhaite que ce paquet appartienne à la « classe de service strictement ordonné ». Les paquets appartenant à cette classe doivent toujours être relayés dans le même ordre qu'ils ont été reçus. En réalité, les AP ne changent pas l'ordre des paquets unicast qu'ils reçoivent, mais il peut arriver qu'ils relaient en premiers des paquets unicast pourtant arrivés après des paquets broadcast (ou multicast). Si le protocole transporté par ce paquet WiFi utilise un mélange d'unicast et de broadcast et que l'ordre de ces paquets est important, alors ce bit devra être égal à 1. Toutefois, la plupart du temps, ce bit est égal à 0 car rares sont les protocoles pour lesquels cela change quoi que ce soit.

3.7.2 Les types de paquets

Il existe trois types de paquets, comme nous l'avons dit :

- **les paquets de gestion (type 0)** sont échangés comme des paquets de données, mais ils servent purement à la couche MAC et ne sont pas « remontés » aux couches réseaux supérieures. Ils mettent en œuvre certaines fonctions du WiFi telles que l'association, l'authentification, les balises, etc. ;
- **les paquets de contrôle (type 1)** sont émis, comme leur nom l'indique, pour contrôler les communications et permettre un bon partage des ondes ;
- **les paquets de données (type 2)** transportent les paquets fournis par les couches réseaux supérieures.

Les paquets de gestion

Voici la liste des paquets de gestion définis dans le 802.11 :

Sous-type	Description
0	Requête d'association
1	Réponse d'association
2	Requête de réassociation
3	Réponse de réassociation
4	Requête de sondage
5	Réponse de sondage
6-7	Inutilisés
8	Balise
9	ATIM
10	Désassociation
11	Authentification
12	Désauthentification
13-15	Inutilisés

Nous avons vu plus haut que tout paquet WiFi pouvait transporter jusqu'à 2 312 octets de données. Les paquets de gestion exploitent ce champ pour transporter divers paramètres. Par exemple, une trame balise indique le temps écoulé depuis l'allumage de l'AP (en microsecondes, codé sur 64 bits), l'intervalle de temps avant la balise suivante et optionnellement le SSID ou encore les paramètres d'économie d'énergie (TIM ou DTIM).

Pour cela, le 802.11 utilise un format de paquet très flexible pour les paquets de gestion : chacun contient d'abord un certain nombre de paramètres obligatoires qui

dépendent du sous-type. Par exemple, les paramètres obligatoires des balises sont le temps écoulé, l'intervalle avant la prochaine balise et enfin un paramètre contenant une série de bits qui indiquent si la balise provient d'un AP (mode Infrastructure) ou d'une station (mode Ad Hoc), ou encore si l'AP prend en charge telle ou telle option, comme par exemple le WEP ou le préambule court.

Ensuite, des paramètres optionnels peuvent être rajoutés : on les appelle des « éléments ». Un élément est composé d'un octet qui indique son type, suivi d'un octet indiquant sa taille (en octets), puis sa valeur. Par exemple, dans une balise, le SSID est un élément. Il peut être présent, ou non. Grâce à cette notion d'élément, les trames de gestion peuvent contenir uniquement les paramètres nécessaires, ce qui les rend assez petites et rapides à échanger.

En outre, ce mécanisme peut être utilisé par des constructeurs pour rajouter des paramètres qui leurs sont spécifiques. Par exemple, un constructeur donné peut rajouter un élément qui indique la charge de l'AP : les stations du même constructeur pourront alors prendre ce paramètre en compte pour choisir le meilleur AP auquel s'associer. Heureusement, les stations provenant d'autres constructeurs ne seront pas gênées : en effet, le type et la longueur de l'élément étant indiqués au début de chaque élément, si une station tombe sur un type qu'elle ne connaît pas, il lui suffit de l'ignorer et de passer à l'élément suivant.

Cette flexibilité permet également au 802.11 de rajouter de nouveaux paramètres aux trames de gestion, tout en conservant une compatibilité complète avec les équipements plus anciens.

Les paquets de contrôle

Voici la liste des paquets de contrôle :

Sous-type	Description
0-9	Inutilisés
10	PS-Poll
11	RTS
12	CTS
13	ACK
14	CF-End
15	CF-End et CF-ACK

Les paquets de contrôle sont extrêmement simples et courts. Ils ne transportent pas de données et ne comportent qu'une ou deux adresses.

Les paquets de données

Pour finir, voici la liste des paquets de données :

Sous-type	Description
0	Données (c'est-à-dire un MPDU)
1	Données et CF-ACK
2	Données et CF-Poll
3	Données, CF-ACK et CF-Poll
4	Paquet vide (sans données)
5	CF-ACK
6	CF-Poll
7	CF-ACK et CF-Poll
8-15	Inutilisés

On voit que certaines fonctions peuvent être regroupées en une seule. Par exemple, en mode DCF, l'AP peut donner la parole à une station (CF-Poll) tout en lui transférant un MPDU, pour éviter de faire deux allers-retours. De même, la station peut acquiescer (CF-ACK) tout en envoyant un MPDU. Les « paquets de données » sans données (CF-Poll, CF-ACK...) sont un peu paradoxaux, mais ils sont placés dans cette catégorie pour plusieurs raisons : d'une part, il ne restait plus beaucoup de place parmi les paquets de gestion et d'autre part, puisque les paquets « Données et CF-xxx » sont dans cette catégorie, autant y mettre également les paquets « CF-xxx ». Enfin, le paquet vide peut servir à vérifier le temps de latence sans envoyer de données.

3.7.3 Les couches supérieures

Les paquets de données encapsulent des paquets issus des couches réseaux supérieures. Par exemple, si vous téléchargez une page web, vous utilisez le protocole HTTP qui véhicule des pages HTML. Le paquet HTTP est encapsulé dans un paquet TCP, lui-même encapsulé dans un paquet IP, lui-même encapsulé dans un paquet LLC. Ce paquet LLC est notre MSDU : il sera éventuellement fragmenté en plusieurs MPDU, s'il est trop gros. Nous y sommes enfin : ces MPDU sont nos paquets de données WiFi !

Un MSDU commence donc en général par un en-tête LLC, suivi d'un en-tête IP. Si le protocole HTTP est utilisé, l'en-tête IP sera suivi d'un en-tête TCP et pour finir le paquet HTTP lui-même. Si l'on utilise un protocole basé sur TCP (les plus fréquents), alors les données proprement dites seront précédées, dans une trame WiFi, par plus de 70 octets d'en-têtes variés (en comptant l'en-tête MAC)... sans compter le préambule et l'en-tête PLCP (voir le chapitre 2). C'est l'une des raisons pour lesquelles le débit réel (observé par l'utilisateur) est beaucoup plus faible que le débit théorique (débit au niveau physique).

3.8 LES AMÉLIORATIONS DU 802.11N

Nous avons vu au chapitre précédent que le 802.11n apporte plusieurs nouveautés dans le WiFi au niveau de la couche physique, notamment le MIMO et la possibilité d'utiliser des canaux de 40 MHz au lieu de 20 MHz. Ceci permet d'augmenter à la fois le débit et la portée du WiFi. Mais le 802.11n améliore également le débit par le biais de deux optimisations de la couche MAC : l'agrégation de trames et les acquittements groupés.

3.8.1 L'agrégation de trames

Il y a toujours des délais entre les trames WiFi (voir § 3.2), et en outre chacune comporte un en-tête de taille fixe. Donc si ces trames transportent peu de données, on peut facilement se retrouver dans une situation où l'on passe plus de temps à attendre entre les trames et à transmettre des en-têtes qu'à envoyer des données. Autrement dit, plus les trames sont petites, plus on gaspille de la bande passante. Afin d'augmenter le débit, le 802.11n propose donc deux solutions alternatives qui permettent d'augmenter la taille des trames, en regroupant plusieurs trames en une seule : l'A-MSDU et l'A-MPDU (*Aggregated MSDU/MPDU*, c'est-à-dire « *MSDU/MPDU agrégé* »).

La solution A-MSDU consiste à regrouper plusieurs trames possédant la même source, la même destination et la même classe de trafic WMM (le cas échéant) en une longue trame agrégée : pour cela, les données de ces trames sont collées les unes à la suite des autres (sans leurs en-têtes), et un seul en-tête et un seul code d'intégrité (CRC) est rajouté à l'ensemble. Tandis qu'une trame normale peut contenir jusqu'à 2 304 octets de données (plus éventuellement les octets nécessaires au cryptage, cf. § 3.7.1), la taille d'une trame agrégée A-MSDU peut atteindre 8 kilo-octets, soit 8 192 octets (plus les octets nécessaires au cryptage). La solution A-MSDU permet ainsi de réduire considérablement la perte de temps entre les trames, et le temps passé à transmettre des en-têtes. Malheureusement, elle a un gros inconvénient : puisque les trames agrégées sont plus longues, le risque qu'une erreur s'y glisse pendant la transmission est très importante : on doit alors renvoyer toute la trame agrégée ! Dans un environnement bruité, on risque ainsi de perdre plus de bande passante à renvoyer les trames agrégées mal transmises que ce que l'A-MSDU permet de gagner avec la diminution du nombre d'en-têtes et de l'espace entre les trames. C'est pourquoi les points d'accès 802.11n adaptent généralement la taille des trames agrégées A-MSDU en fonction des conditions.

La solution A-MPDU consiste également à agréger des trames qui ont la même source, la même destination et la même classe de trafic WMM. Cependant cette fois-ci les trames sont simplement collées bout à bout et envoyées en un seul bloc (la trame agrégée A-MPDU). La quantité maximale de données que peut contenir une trame agrégée A-MPDU est de 64 Ko, soit 65 536 octets (plus les octets nécessaires au cryptage). Le risque qu'une erreur se glisse dans cette trame agrégée est très important, mais heureusement chaque trame contenue dans la trame agrégée contient toujours son propre en-tête et surtout son propre code de contrôle d'intégrité (CRC), ce qui permet au destinataire, en cas d'erreur de transmission, de rejeter uniquement la (ou

les) trame(s) défectueuse(s), et non l'ensemble de la trame agrégée. En environnement peu bruité, l'A-MSDU est un peu plus efficace que l'A-MPDU, car il supprime les en-têtes des trames ; mais inversement, en environnement bruité, l'A-MPDU est plus efficace car il limite les répétitions.

3.8.2 Acquittements groupés

À chaque fois qu'une station WiFi émet un paquet, elle attend en retour un paquet ACK (« *acknowledgement* », c'est-à-dire acquittement, cf. § 3.2.1). Ce paquet ACK occupe donc une part non négligeable de la bande passante.

Le 802.11n optimise donc la couche MAC du WiFi en réduisant d'une part la taille du paquet ACK, qui passe de 128 octets à 8 octets, et surtout en permettant à une station d'émettre plusieurs trames, puis d'attendre un acquittement groupé, qu'on appelle le « *Block-ACK* »[1]. On économise ainsi un peu de bande passante. Ceci est particulièrement utile lorsque l'on met en œuvre l'agrégation de trames. Par exemple, au lieu d'émettre trois trames en attendant à chaque fois un ACK, soit en tout 6 trames émises, on peut émettre une seule trame agrégée A-MPDU et recevoir un seul Block-ACK.

Résumé

Au cours de ce chapitre, nous avons présenté la couche MAC du protocole 802.11, ses principales fonctions et le format de ses paquets. Pour cela, nous avons commencé par situer la couche MAC : entre les couches physiques et la couche LLC (802.2).

Un bref rappel sur l'Ethernet nous a ensuite permis d'aborder le CSMA/CD, qui est une stratégie de partage du média très simple : un délai d'attente aléatoire permet de répartir plus ou moins équitablement la parole entre les stations. Cette stratégie perd de son efficacité lorsque le nombre de stations cherchant à communiquer en même temps est élevé : des « collisions » sont alors fréquentes. Nous avons alors pu aborder le partage des ondes défini par la norme 802.11 : la première stratégie s'appelle le DCF et repose sur le CSMA/CA et le mécanisme RTS/CTS. Le CSMA/CA est une variante du CSMA/CD dans laquelle chaque station envoie un accusé de réception (ACK) pour tout paquet reçu. Avec le mécanisme RTS/CTS, une station demande la parole avant d'envoyer un paquet (si sa taille dépasse un seuil fixé), ce qui permet de réduire les collisions entre les stations qui ne sont pas à portée les unes des autres. Nous avons ensuite abordé la stratégie PCF (optionnelle et peu répandue), dans laquelle l'AP donne successivement la parole à chaque station, ce qui permet d'améliorer la fluidité du trafic. Une meilleure gestion de la qualité de service (QoS) est possible grâce au 802.11e, qui définit les stratégies EDCF et EPCF : il s'agit d'améliorations du DCF et du PCF, qui font intervenir la notion de classe

1. Le principe du Block-ACK a été défini dans le standard 802.11e, mais n'a que peu été utilisé. Il a été amélioré par le 802.11n, et est maintenant bien plus souvent mis en œuvre.

de trafic (TC). L'EDCF permet ainsi de donner une priorité plus ou moins grande à chaque TC (e-mails, voix sur IP...), tandis que l'EPCF va plus loin, en permettant à l'AP de coordonner intelligemment le partage des ondes entre les stations, avec des règles précises pour chaque TC (bande passante garantie, fluidité...). La certification WMM de la WiFi Alliance correspond aux produits respectant l'EDCF.

La certification *WMM-Scheduled Access* correspond aux produits à la norme EPCF.

Par ailleurs, nous avons présenté les deux topologies 802.11 définies par la couche MAC : les réseaux de type Infrastructure où les stations communiquent avec le réseau *via* un point d'accès (chaque réseau sans fil étant identifié par un SSID) et les réseaux de type Ad Hoc où toutes les stations communiquent directement les unes avec les autres. Malheureusement, le mode Ad Hoc ne définit pas comment deux stations peuvent communiquer par le biais d'une troisième : les réseaux maillés en mode Ad Hoc font l'objet de la norme 802.11s.

Nous avons détaillé le processus d'association : chaque AP envoie régulièrement des trames balises pour signifier sa présence et assurer la synchronisation des stations. Les stations peuvent détecter un réseau sans fil grâce à ces balises, ou bien en envoyant des requêtes de sondage (*probe*). Une fois le réseau détecté, la station doit s'authentifier. Il y a deux modes d'authentification 802.11 : le mode « ouvert » et le mode « WEP ». Le premier accepte toute station qui le demande, le second suppose la configuration d'une même clé WEP dans tous les AP et stations du réseau. Une fois authentifiée, une station n'a plus qu'à envoyer une requête d'association pour rejoindre le réseau. En mode Ad Hoc, rien de tout ceci n'est nécessaire : une station peut d'office communiquer avec toutes les autres à sa portée.

Nous avons alors abordé rapidement les principales mesures de sécurité du WiFi : masquer le SSID, filtrer les stations par leur adresse MAC, utiliser le cryptage WEP, ou mieux, utiliser le WPA ou WPA2. Nous approfondirons toutes ces solutions dans les chapitres 6 à 10.

Enfin, nous avons également présenté :

– le contrôle d'erreur, assuré par un code CRC, calculé à partir du paquet et rajouté à la fin de celui-ci ;

– la fragmentation et le réassemblage des paquets, permettant de résister à un environnement bruyant ;

– l'acheminement des paquets, notamment lorsque des AP sont reliés entre eux, sans fil (WDS) ;

– l'économie d'énergie : rendue possible grâce à la synchronisation des stations et des messages prévus à cet effet (PS-Poll...), et optimisée pour la QoS avec le WMM-PS.

Nous avons ensuite détaillé le format des paquets WiFi : les paquets de données (MPDU), les paquets de contrôle (RTS, CTS, ACK...) et les paquets de gestion (association, authentification...).

Pour finir, nous avons présenté les améliorations de la couche MAC apportées par le 802.11n pour améliorer le débit : l'agrégation de trames et les acquittements groupés (Block-ACK).

DEUXIÈME PARTIE

Déploiement

Cette partie est dédiée au déploiement des réseaux WiFi. Elle est composée de deux chapitres :

- le chapitre 4 présente le matériel WiFi dans son ensemble et permet de connaître les paramètres à prendre en compte pour effectuer un bon choix. Sont présentés les adaptateurs WiFi, les AP, les périphériques WiFi tels que les imprimantes ou les téléphones WiFi, les antennes et d'autres produits liés au WiFi ;
- le chapitre 5 traite de la couverture radio, pour permettre un bon déploiement des AP, en fonction de l'objectif : connexion de point à point, réseau d'entreprise simple ou à haute capacité, environnement bruyant ou non, etc.

4

Le matériel

Objectif

Ce chapitre a pour but de présenter les principaux types de produits WiFi disponibles aujourd'hui. Des adaptateurs PCMCIA, PCI, USB, voire de petits AP connectés au port Ethernet, permettent à vos ordinateurs de se relier au réseau WiFi. Les points d'accès peuvent être de simples répétiteurs, des ponts sophistiqués, des routeurs ou encore des contrôleurs d'accès complets : ils sont les briques de votre réseau sans fil. De plus en plus d'ordinateurs portables et bien d'autres équipements informatiques sont maintenant vendus avec un adaptateur WiFi intégré : des smartphones, des imprimantes, des scanneurs, des caméras de vidéosurveillance, etc. Pour finir, des antennes peuvent être branchées à la majorité des points d'accès et des adaptateurs WiFi afin de concentrer le signal radio dans certaines directions et réaliser une couverture plus efficace. Ce chapitre doit vous permettre de comprendre le rôle et les fonctions de chaque type de matériel, afin de vous aider à bien le choisir et peut être vous donner des idées sur quelques applications inattendues du WiFi.

4.1 LES ADAPTATEURS

4.1.1 Le rôle de l'adaptateur

L'adaptateur WiFi est le composant matériel qui permet à un équipement quelconque de communiquer en WiFi. Par exemple, pour fonctionner, un AP utilise un adaptateur WiFi (voire plusieurs). Dans certains AP, l'adaptateur peut même être détaché et remplacé, ce qui permet de l'adapter à une nouvelle norme WiFi, telle que le 802.11n ou le 802.11i, sans avoir à changer tout l'AP.

Un adaptateur est composé d'une antenne radio et d'un processeur mettant en œuvre la norme 802.11. Certains adaptateurs WiFi sont capables de gérer plusieurs radios : par exemple l'une à 2,4 GHz en 802.11b(g) et l'autre à 5 GHz en 802.11n. Dans certains cas, on peut (ou on doit) brancher une antenne externe.

> Pour connecter en WiFi un ordinateur portable ou fixe qui n'intègre pas un adaptateur, il est nécessaire de brancher un adaptateur WiFi.

4.1.2 La connectique

Des formats variés

Il existe des adaptateurs WiFi pour tous les goûts : certains sont présentés sous la forme de cartes externes pouvant être branchées à un port de type PCMCIA ou à un port Compact Flash. Certains adaptateurs sont des cartes destinées à être branchées à l'intérieur d'un ordinateur, sur un port PCI, Mini-PCI ou ISA. D'autres se présentent sous la forme de boîtiers ou bâtonnets (*dongle* ou *stick*) connectés au port USB ou FireWire d'un ordinateur fixe ou portable. De petits AP « ponts » (voir paragraphes suivants), peuvent servir d'adaptateur WiFi à brancher sur le port Ethernet d'un ordinateur. Enfin, certains adaptateurs sont conçus spécialement pour être « embarqués » dans des ordinateurs portables qui intègrent la technologie WiFi (par exemple les ordinateurs portables Centrino d'Intel), dans des modules spécifiques à certains PDA, dans des AP, ou encore dans des machines industrielles, résistant à la température, aux chocs, à l'humidité ou encore aux interférences.

Figure 4.1 — Les adaptateurs WiFi.

Quel adaptateur choisir ?

Chaque type d'adaptateur a ses propres avantages et est donc mieux adapté à un usage donné. Les cartes PCMCIA ou Compact Flash sont pratiques à transporter et le branchement est assez fiable, mais elles ne peuvent pas être connectées à un ordinateur fixe (à moins que celui-ci soit équipé d'un port adapté, ce qui n'est en général pas le cas).

Les *dongles* USB sont souvent moins pratiques à transporter car ils sont reliés à l'ordinateur par un câble USB. Quelques petits sticks USB n'ont pas de câble et sont branchés directement sur le port USB, mais en situation de mobilité, cette connexion est parfois précaire. L'avantage de l'USB est surtout que le même dongle WiFi peut être branché sur un ordinateur fixe ou portable, car ces derniers ont maintenant tous (ou presque) des ports USB.

Les cartes internes (PCI, Mini-PCI et ISA) sont surtout utiles quand on veut relier un ordinateur fixe à un réseau WiFi ou intégrer le WiFi dans un ordinateur portable de façon permanente. L'inconvénient est qu'il faut ouvrir le boîtier de l'ordinateur pour installer la carte, ce qui est délicat et prend du temps.

Les adaptateurs Ethernet sont trop volumineux pour être transportés systématiquement avec soi. En outre, ils doivent souvent être branchés à une prise électrique ce qui n'arrange rien. Notons toutefois que certains adaptateurs de ce type peuvent être branchés à un port USB pour assurer leur alimentation électrique. Bref, ils ne sont pas conçus pour la mobilité. Cependant, ils sont particulièrement utiles pour connecter des visiteurs à un réseau WiFi sans avoir à reconfigurer quoi que ce soit dans leur ordinateur : en leur fournissant un adaptateur Ethernet, ils se connectent au réseau sans fil à travers une connexion filaire classique et n'ont aucun paramètre WiFi à configurer : ils n'ont même pas à sélectionner un SSID, car celui-ci est configuré à l'avance dans l'adaptateur. C'est un produit très apprécié des hôteliers : lorsqu'un client dépourvu d'adaptateur WiFi souhaite se connecter au *hotspot* de l'hôtel, on peut lui proposer un adaptateur Ethernet, qui lui permettra de se connecter sans avoir à reconfigurer son poste.

Le firmware

Les fonctions de l'adaptateur qui doivent être très performantes sont en général mises en œuvre par des composants électroniques spécialisés. C'est souvent le cas, par exemple, de l'algorithme de cryptage RC4 sur lequel repose le WEP (voir le chapitre 7).

Cependant, de nombreuses fonctions 802.11 sont réalisées par un micro-programme (*firmware*) situé dans l'adaptateur. L'avantage du *firmware* est qu'il peut en général être mis à jour, ce qui permet de rajouter de nouvelles fonctions sans changer de matériel. Par exemple, de nombreux adaptateurs peuvent être simplement mis à jour de cette façon pour pouvoir gérer le *Wireless Protected Access* (WPA).

Avant de choisir un adaptateur, renseignez-vous sur ses capacités d'évolution : possède-t-il un *firmware* pouvant être mis à jour ? Le constructeur fournit-il fréquemment des mises à jour ? Quelles fonctions pourront être mises à jour ?

4.1.3 Le pilote

Une interface pour le système d'exploitation

À part pour les adaptateurs WiFi Ethernet, il est en général nécessaire d'installer sur son ordinateur le pilote (*driver*) de l'adaptateur WiFi. Le pilote permet au système d'exploitation de savoir comment communiquer avec l'adaptateur. Il est en général fourni sur un CD-ROM accompagnant le produit. Avant l'achat, assurez-vous que les systèmes d'exploitation pour lesquels le pilote a été conçu vous conviennent. Il existe ainsi des adaptateurs WiFi qui ne possèdent des pilotes que pour certaines versions de Windows, ou pour Windows et Linux et plus rarement pour Windows, Linux et Mac OS.

N'hésitez pas à consulter l'Internet pour essayer d'avoir des témoignages de clients sur la qualité du produit, sa stabilité et sa facilité d'installation. C'est d'ailleurs un conseil général pour tout produit !

Une interface pour l'utilisateur

Outre les outils de gestion du périphérique par le système d'exploitation, le pilote fournit en général une interface d'utilisation pour l'utilisateur ainsi que des outils de configuration avancée. L'interface d'utilisation doit être aussi claire que possible car elle sera utilisée fréquemment (fig. 4.2).

La plupart des adaptateurs permettent de détecter et d'afficher, en un ou deux clics de souris, la liste des réseaux sans fil disponibles, c'est-à-dire ceux dont l'identifiant est diffusé (le SSID, voir § 3.3.1). L'utilisateur peut sélectionner le SSID de son choix dans cette liste ou bien saisir manuellement un SSID, si celui-ci est caché et n'apparaît pas dans la liste. Certains pilotes indiquent le BSSID ou le canal de l'AP le plus proche ou d'autres informations utiles. L'utilisateur peut en général choisir un SSID préféré (ou une liste de SSID) auquel le pilote s'associera dès qu'il sera à portée de signal. Bref, il s'agit de l'interface centrale pour l'utilisateur. Certaines sont très complètes et intuitives, d'autres pas du tout : essayez de vous renseigner avant l'achat car c'est un point assez important pour la facilité d'utilisation.

Quoi qu'il en soit, si vous utilisez Windows XP, il faut savoir qu'une interface par défaut, appelée « Zéro Config », peut souvent être utilisée en remplacement (ou parfois en complément) de l'interface fournie avec le pilote de l'adaptateur. L'interface Zéro Config est assez sommaire (fig. 4.3) mais elle est pratique et fonctionnelle : elle permet de détecter les réseaux sans fil, de s'associer au réseau de son choix, de définir une liste de réseaux préférés et de saisir des paramètres de configuration de sécurité WEP ou 802.1x. Après le téléchargement et l'installation des mises à jour adéquates[1] de Windows, le WPA est également pris en charge par l'interface Zéro Config.

De même Windows Vista et tous les systèmes d'exploitation récents disposent d'une interface par défaut pour gérer la connexion WiFi, que l'on peut utiliser en complément ou en remplacement de l'interface fournie avec l'adaptateur.

1. Les mises à jour Q815485 et KB826942 sont inclues dans le Service Pack 2 de Windows XP.

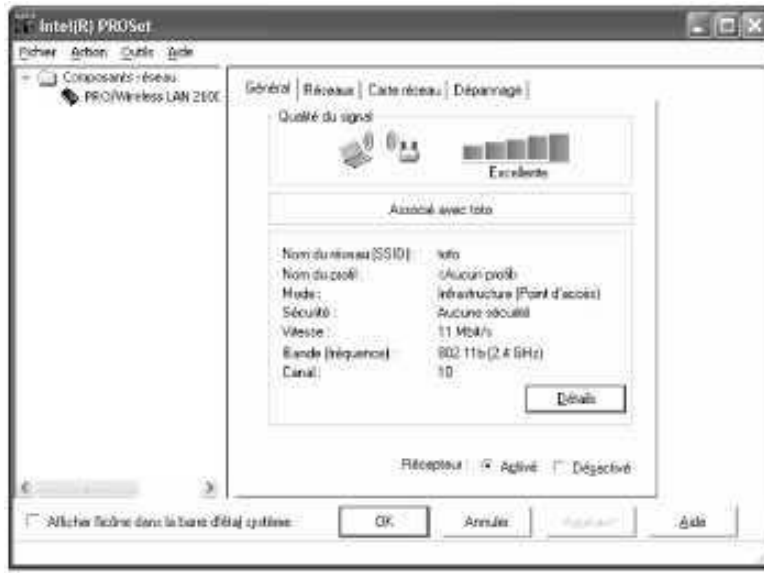


Figure 4.2 — Exemple de l'interface Intel PROSet.

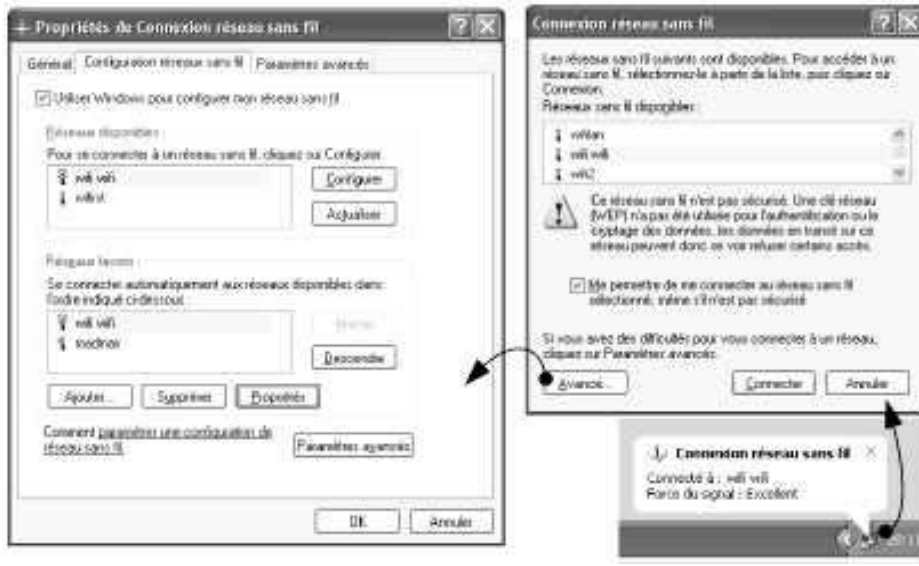


Figure 4.3 — L'interface Zero Config intégrée dans Windows XP.

Les réglages avancés

Le pilote de l'adaptateur permet souvent de manipuler des paramètres 802.11 avancés tels que l'activation de l'économie d'énergie, la puissance d'émission, la sensibilité, le RTS *Threshold* (voir le chapitre 3), etc. Certains adaptateurs peuvent être configurés en mode *monitor*, très utile pour « sniffer » (c'est-à-dire écouter) et analyser un réseau

sans fil sans même avoir à s'y connecter. Quelques adaptateurs sont même fournis avec de véritables outils d'analyse de réseau sans fil.

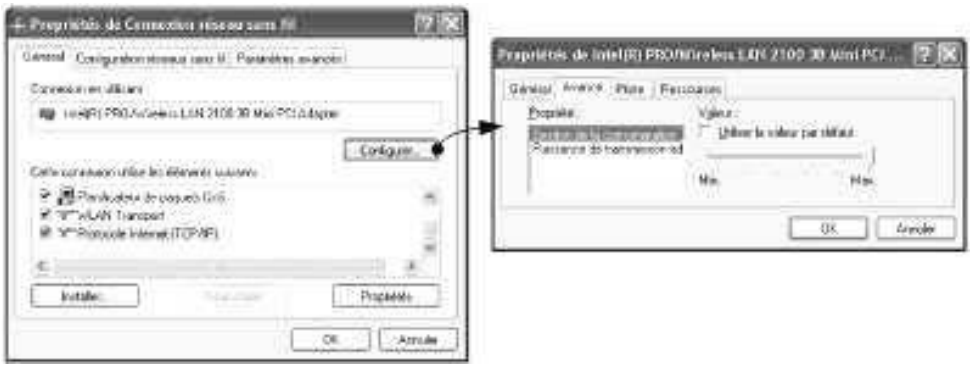


Figure 4.4 — Configuration avancée : exemple avec un adaptateur Centrino sous Windows XP.

4.2 LE POINT D'ACCÈS

Comme nous l'avons vu au chapitre 2, les points d'accès (AP) sont le cœur d'un réseau sans fil de type Infrastructure. Ils gèrent de nombreuses fonctions telles que l'authentification et l'association des stations, ou encore l'acheminement des paquets WiFi entre les stations associées. D'autres fonctions sont optionnelles mais très fréquentes, par exemple :

- la gestion du *hand-over* : un utilisateur peut alors passer sans déconnexion d'un AP à un autre. Pour cela, les AP concernés doivent communiquer entre eux *via* le système de distribution (DS) qui est le plus souvent un réseau filaire ;
- le filtrage des périphériques autorisés, en fonction de leur adresse MAC ;
- le cryptage des données échangées et l'authentification des périphériques grâce aux protocoles WEP, WPA ou WPA2.

En plus de ces fonctions WiFi, toutes sortes de services de plus haut niveau peuvent être rajoutés. Ce sont ces fonctions qui déterminent dans quelle catégorie un point d'accès se situe : pont, routeur, contrôleur d'accès, etc.

4.2.1 Le pont vers un réseau filaire

Le rôle d'un pont

Les ponts WiFi (*bridge*) permettent aux périphériques sans fil de se connecter à un réseau filaire (en général Ethernet) : ils se contentent pour cela de relayer les paquets reçus sur l'interface WiFi (on parle de « port WLAN ») en paquets adaptés au réseau filaire (*via* le « port LAN ») et *vice versa*. Les ponts simples se situent donc au niveau

de la couche OSI numéro 2 : en particulier, ils ne s'occupent pas de routage IP[1] (couche 3).

Notons que le réseau filaire est en général utilisé comme système de distribution pour gérer le *hand-over* entre plusieurs AP d'un même réseau sans fil.

Figure 4.5 — Exemple de pont 802.11g/Ethernet[2].

L'apprentissage automatique

La grande majorité des ponts est capable d'optimiser les échanges de paquets de la façon suivante : pour chaque paquet qui transite par lui, le pont regarde sur quel port ce paquet est arrivé (WLAN ou LAN) ainsi que l'adresse MAC du périphérique qui l'a émis. Il « apprend » donc automatiquement de quel côté se trouve chaque périphérique du réseau, au fur et à une mesure que les paquets passent : côté filaire ou côté sans fil. De cette façon, lorsqu'un AP pont reçoit un paquet du côté LAN, il ne le relaie du côté WLAN que si ce paquet a pour destinataire une station située du côté WLAN. Inversement, s'il reçoit un paquet côté WLAN, il ne le relaie du côté LAN que si nécessaire. Ceci permet d'éviter de retransmettre le trafic inutilement.

La plupart des ponts apprennent automatiquement de quel côté se situe chaque station, afin de ne pas transférer de paquets inutilement.

Prenons un exemple concret pour bien comprendre l'intérêt de cette optimisation : imaginons un réseau d'entreprise composé d'une cinquantaine de postes reliés entre eux par le biais d'un réseau filaire Ethernet. En outre, trois ou quatre postes sont connectés au réseau *via* un pont WiFi. La majorité du trafic sur le réseau a lieu entre les postes du réseau filaire. Puisqu'il s'agit d'un réseau Ethernet, tout le trafic est reçu par l'ensemble des équipements du réseau, dont le pont. Si celui-ci se contentait d'envoyer ce trafic dans les airs, cela occuperait l'essentiel de la bande passante du WiFi. Grâce à l'apprentissage automatique, au contraire, seul le trafic qui concerne les postes connectés en WiFi transitera effectivement par les airs.

1. Si vous n'êtes pas familier avec le routage IP, nous vous invitons à consulter sur *www.livrewifi.com* l'annexe A qui offre une vue d'ensemble des réseaux IP.

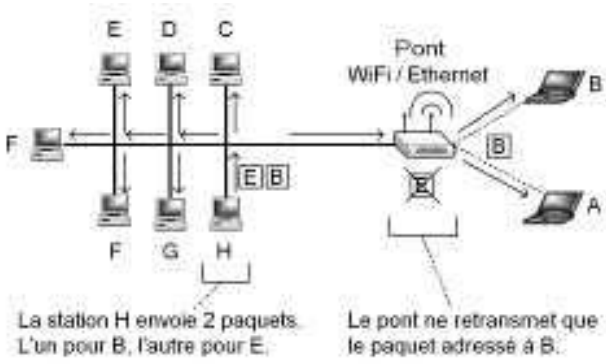


Figure 4.6 — L'apprentissage automatique des ponts.

Notons que ce mécanisme n'a rien de spécifique au WiFi : par exemple, il existe des ponts qui relient deux portions d'un même réseau Ethernet et ils fonctionnent de la même manière. Ils servent alors à diminuer l'encombrement sur le réseau : l'idéal est alors de les placer entre deux portions du réseau qui communiquent rarement entre elles. Imaginez une salle de réunion contenant deux groupes de personnes n'ayant pas les mêmes intérêts : les conversations des uns n'intéresseront que rarement les autres et il sera plus logique de les placer dans deux salles séparées. Le pont peut être vu comme une personne située au milieu et qui sert de relais pour les quelques messages qui doivent être échangés entre les deux salles.

Broadcast et multicast

Il est important de comprendre qu'un pont se situe au niveau de la couche 2 du modèle OSI. Il ne découpe pas un réseau en deux sous-réseaux distincts (*subnets*) mais permet de relier deux portions d'un même réseau. En particulier, si une requête de type *broadcast* (adressée à tout le monde) est émise par une station, alors toutes les stations du réseau la recevront, des deux côtés du pont. Au niveau de la couche 3, toutes les stations seront dans le même sous-réseau IP. Le pont est donc complètement transparent pour les couches réseau supérieures à 2.

Le cas du trafic multicast est un peu plus compliqué puisque le destinataire d'un paquet est un groupe et non une seule station. La façon la plus simple de gérer le trafic multicast, pour un pont, est de le traiter exactement comme du trafic broadcast. Pour cela, rien de plus simple, il suffit de le retransmettre sur chaque port. Le trafic multicast peut être détecté facilement car le premier octet de l'adresse MAC de destination est impair (le dernier bit du premier octet est égal à 1). Malheureusement, ce n'est pas la façon la plus optimale de gérer la bande passante : si personne n'est intéressé par le trafic multicast en question sur une branche du réseau, à quoi bon le retransmettre vers cette branche ? Les ponts les plus sophistiqués ont un mécanisme d'apprentissage « intelligent » pour le multicast : ils détectent sur quels ports se trouvent les membres d'un groupe donné et ne retransmettent le trafic multicast de ce groupe que vers ces ports. Pour cela, la principale méthode consiste à détecter les stations qui demandent

à rejoindre ou à quitter un groupe multicast particulier. Ces requêtes reposent sur l'*Internet Group Management Protocol* (IGMP) qui est un protocole de la couche 3.

Isolation des stations sans fil

Certains AP proposent une option d'isolation des stations WiFi : si cette option est activée, tous les paquets provenant d'une station WiFi et à destination d'une autre station WiFi seront éliminés par l'AP. Ceci est particulièrement utile dans un *hotspot*, afin d'éviter que les clients ne se « voient » entre eux. Sans cette option, un pirate peut simplement s'associer au *hotspot* et communiquer alors avec tous les clients connectés. Sous Windows, par exemple, il verra les autres postes dans le « voisinage réseau » et il pourra consulter les éventuels répertoires partagés des voisins !

En entreprise, cette option est en général désactivée car on veut que les stations sans fil puissent communiquer entre elles, une fois qu'elles ont été identifiées et qu'elles se sont associées à un AP.

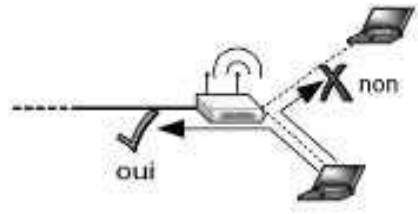


Figure 4.7 — Point d'accès configuré pour isoler les stations sans fil.

4.2.2 Le point d'accès répétiteur

Principe de fonctionnement

Comme nous l'avons vu au chapitre 2, certains AP sont capables de se connecter sans fil à un autre AP pour rejoindre le système de distribution (*Distribution System*, DS) et le réseau filaire. Cela signifie qu'un AP peut étendre la couverture d'un réseau sans fil sans même qu'il soit nécessaire de le relier au réseau filaire ! On appelle souvent ce mode de connexion sans fil le mode *bridge*, ce qui peut entraîner une confusion avec les ponts WiFi vers un réseau filaire que nous avons décrits au paragraphe précédent. Aussi, il est préférable de les appeler les « AP répétiteurs »[1].

Dans la pratique, un AP répétiteur doit en général être configuré avec les adresses MAC des AP par lesquels il peut passer pour atteindre le DS. Certains produits peuvent gérer un seul relais, d'autre quatre ou six, voire davantage.

1. Les répétiteurs WiFi les plus simples sont des antennes actives qui amplifient le signal électromagnétique qu'elles reçoivent. Elles ne sont que très rarement utilisées car les AP répétiteurs ne sont finalement pas tellement plus chers et offrent bien plus de fonctionnalités.

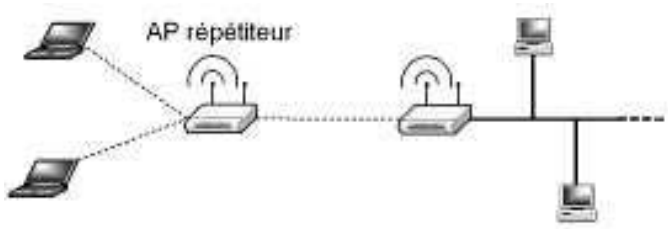


Figure 4.8 — Le point d'accès répétiteur.

Le principal inconvénient d'un AP répétiteur provient du fait qu'il fonctionne en général sur un seul canal : il utilise le même canal pour communiquer avec les autres AP et avec les stations qui lui sont associées. Ainsi lorsqu'une station envoie un paquet *via* l'AP auquel elle est associée, ce paquet est réémis vers l'AP suivant sur le même canal : résultat, la bande passante est divisée au moins par deux à chaque saut !

La solution à ce problème réside dans l'utilisation d'un canal différent pour la fonction d'AP et la fonction de relais sans fil. Ceci nécessite deux circuits radio et les produits coûtent donc nettement plus cher. En contrepartie, on ne perd que peu de bande passante à chaque saut.

> Si un AP répétiteur utilise le même canal pour communiquer avec les stations et avec l'AP auquel il est relié, le débit est divisé par deux.

Les premières offres

Malheureusement, le standard 802.11 n'est pas très précis sur la façon de procéder pour mettre en œuvre des relais sans fil entre AP, en conséquence les solutions sont souvent « propriétaires », c'est-à-dire qu'elles varient d'un constructeur à l'autre et elles ne fonctionnent que rarement les unes avec les autres.

Les plus anciennes utilisaient une technique appelée le MAC *Masquerading* : lorsqu'un client associé à un AP répétiteur envoie un paquet, l'AP répétiteur modifie ce paquet pour faire croire au reste du réseau qu'il en est la source : il remplace l'adresse MAC d'origine du paquet (c'est-à-dire l'adresse de la station) par sa propre adresse MAC. Ensuite, il fait suivre ce paquet modifié vers l'AP auquel il est associé. Du point de vue de l'AP « classique », l'AP répétiteur est une station comme une autre. Lorsque la réponse à la requête parvient à l'AP répétiteur, celui-ci modifie la réponse pour la rediriger vers la station initiale : l'adresse MAC de destination du paquet devient celle de la station et le « tour est joué ».

Pour vous faire une idée de ce que cela signifie, imaginez que vous preniez les commandes pour vos amis, dans un bar. Si Jean vous demande une limonade et Marie vous demande un café, au lieu de dire au serveur ce que chacun de vos amis désire, vous affirmez : « *je* veux un café et une limonade ». Lorsque le serveur revient avec la commande, vous devez vous souvenir qui a demandé quoi pour leur distribuer la bonne boisson. L'avantage est que du point de vue du serveur, il n'y a qu'un seul client tout à fait classique à gérer.

Comme vous pouvez l'imaginer, ce mécanisme comporte de très sérieuses failles : d'une part, il suppose que l'AP répétiteur « mémorise » l'origine de chaque requête pour savoir à qui rediriger les réponses. En outre, il faut que l'AP répétiteur soit capable de détecter que tel paquet est bien la réponse à telle requête, ce qui est parfois loin d'être évident. Pour finir, le fait que toutes les stations connectées au travers de l'AP répétiteur apparaissent au reste du réseau comme une seule et même station peut poser de sérieux problèmes de sécurité et poser de gros problèmes avec certains équipements réseaux. Bref, cette solution a le mérite d'avoir été la première à voir le jour, mais elle n'est pas recommandée aujourd'hui.

Le WDS

Depuis début 2003, des produits s'appuyant sur un mécanisme (plus ou moins) défini dans le standard 802.11, appelé le *Wireless Distribution System* (WDS)[1], ont commencé à voir le jour. Non seulement le WDS est beaucoup plus « propre » que les solutions propriétaires, mais l'interopérabilité entre les produits WDS de différents constructeurs est souvent possible. La meilleure garantie que des AP répétiteurs fonctionnent bien ensemble reste toutefois qu'ils proviennent du même constructeur.

Le « routage » entre les AP

La plupart des AP répétiteurs gèrent l'acheminement des paquets à la manière d'un commutateur (*switch*). Un commutateur est un pont à ports multiples : alors qu'un pont possède deux ports et relie entre elles deux portions d'un même réseau, le commutateur possède *n* ports et relie *n* portions d'un réseau. La majorité des commutateurs appliquent la même logique d'apprentissage que celle décrite plus haut pour les ponts : en observant l'adresse MAC d'origine des paquets et le port sur lequel ils arrivent, ils « apprennent » progressivement sur quel port il faut envoyer les paquets pour atteindre chaque périphérique.

Les AP répétiteurs fonctionnent de cette façon : chaque lien sans fil avec un autre AP est considéré comme un port différent. Ce mécanisme permet de bâtir une topologie réseau assez simple.

Malheureusement, ce type de mécanisme est vulnérable aux boucles. Si la topologie mise en place contient des boucles, un paquet peut être transmis à un AP, puis à un second, à un troisième et de nouveau au premier, à l'infini, ce qui annihilera très rapidement toute la bande passante !

En outre, des paquets provenant d'une même station peuvent arriver à un AP sur plusieurs ports différents, ce qui peut « troubler » le mécanisme d'apprentissage automatique de l'AP, qui ne saura pas sur quel port envoyer la réponse.

Avec un AP répétiteur fonctionnant à la façon d'un commutateur, il faut faire attention à s'en tenir à une topologie non redondante, c'est-à-dire sans boucle.

1. Voir le chapitre 3, § 3.6.3.

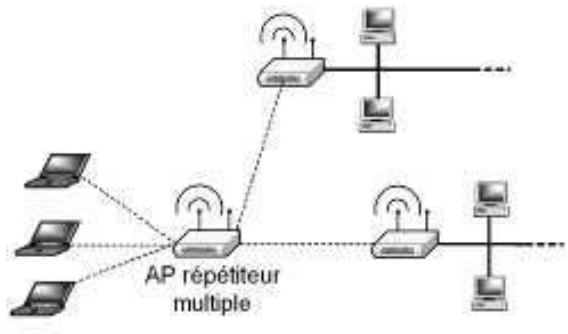


Figure 4.9 — Exemple de topologie sans boucle.

L'infrastructure maillée

Afin d'obtenir une architecture réellement maillée, c'est-à-dire redondante, il est nécessaire de rajouter des mécanismes qui permettent d'éviter les boucles. C'est la raison pour laquelle certains produits WDS utilisent le *Spanning Tree Protocol* (STP) défini par l'IEEE au sein du standard 802.1D.

Le protocole STP est conçu pour les commutateurs du réseau (WiFi ou non). En deux mots, il fonctionne de la façon suivante :

- Au démarrage puis à intervalles réguliers, les commutateurs émettent des paquets STP en multicast sur tout le réseau, afin de détecter les autres commutateurs. La topologie du réseau est ainsi automatiquement déterminée par l'ensemble des commutateurs.
- Ils se coordonnent alors pour élire un commutateur « racine ».
- Chaque commutateur choisit ensuite le meilleur port pour communiquer avec le commutateur racine, de telle sorte que l'arborescence de commutateurs ne contienne aucune boucle et soit aussi efficace que possible.
- Par la suite, tant que la topologie du réseau ne change pas, le trafic ne passe que par les ports sélectionnés.
- Si un commutateur devient indisponible, le processus recommence afin de reconstruire une nouvelle arborescence.
- Tout se passe de façon complètement transparente pour les stations du réseau.

Des algorithmes plus performants

Le mécanisme STP permet d'éliminer le risque de boucles, tout en permettant une redondance en cas de perte d'un lien. Il ne s'agit toutefois pas du mécanisme le plus efficace pour optimiser la bande passante, car une fois l'arbre STP mis en place, il ne change plus (sauf quand un commutateur n'est plus disponible).

Les AP répétiteurs les plus performants mettent en œuvre des algorithmes de routage propriétaires qui prennent en compte, pour l'acheminement de chaque paquet, la charge des AP, la bande passante disponible, le bruit, le chemin le plus court,

etc., de façon à véritablement optimiser le trajet des paquets tout en évitant les boucles. De cette façon, non seulement la redondance du maillage permet de résister à la disparition brutale d'un lien (ce que permet le STP), mais la bande passante est en outre réellement optimisée. Malheureusement, puisqu'il s'agit de solutions propriétaires pour l'instant, tous les AP devront provenir du même constructeur.

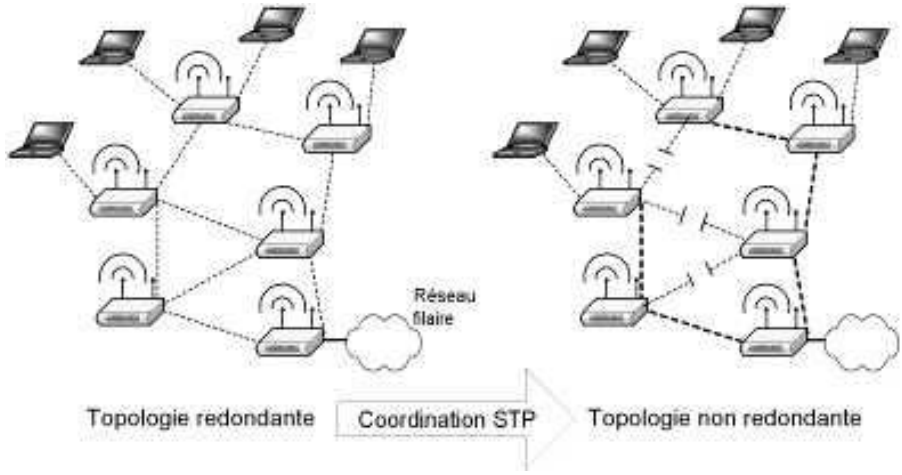


Figure 4.10 — Le *Spanning Tree Protocol* (STP) à l'œuvre.

4.2.3 Les réseaux multiples

Plusieurs infrastructures sans fil

Il peut arriver que l'on souhaite déployer plusieurs services sans fil au même endroit. Par exemple, une société peut déployer un réseau sans fil destiné à ses employés pour l'accès au réseau d'entreprise et un deuxième réseau sans fil (composé d'AP distincts) destiné à permettre aux visiteurs de surfer sur Internet. Pour mettre en œuvre deux services distincts, la solution la plus triviale consiste à déployer deux réseaux sans fil distincts.

Bien sûr, le premier inconvénient de cette solution est son coût : pour chaque service, on doit acheter, installer et configurer un ensemble d'AP distinct. En outre, puisqu'on ne dispose que de trois canaux indépendants en 802.11b et 802.11g (jusqu'à 19 en 802.11a), ce procédé pose rapidement des problèmes d'interférences entre les différents réseaux.

Un simple contrôle d'accès

Une autre solution consiste à déployer un seul réseau sans fil avec un seul SSID et à gérer la différentiation des services au niveau des couches réseau supérieures. C'est ce que permet un contrôleur d'accès (voir le § 4.2.5) : en deux mots, une fois le client associé au réseau et identifié, le contrôleur d'accès ne le laisse utiliser que tel ou tel service réseau : par exemple, un employé pourra accéder à tout le réseau, un visiteur

ne pourra aller que sur Internet, etc. Ce filtrage et routage variable se fait au niveau IP, donc dans la couche 3 du modèle OSI.

Malheureusement, cette solution manque de souplesse et comporte des failles de sécurité. Pour illustrer ceci, reprenons l'exemple de l'entreprise qui souhaite un service pour ses employés et un service pour ses visiteurs. L'entreprise aura grand intérêt à protéger l'accès au réseau d'entreprise avec la sécurité WPA. Mais si elle le fait, les visiteurs auront du mal à se connecter, car la configuration du poste client pour le WPA n'est pas toujours triviale. La plupart des visiteurs auront du mal à se connecter. Mais si l'on désactive le WPA pour faciliter la vie des visiteurs, on compromet la sécurité du réseau d'entreprise. Bref, tous les services ont la même configuration MAC : SSID, sécurité, qualité de service, etc.

Multi-SSID

Depuis 2001, de plus en plus d'AP sont capables de gérer plusieurs SSID. Une fois n'est pas coutume, les produits diffèrent dans la façon de mettre en œuvre cette fonctionnalité, car elle n'est pas clairement définie dans le standard 802.11. Voici les différentes possibilités :

- Plusieurs SSID peuvent être envoyés dans chaque trame balise (*beacon frames*) émise par l'AP. Ceci n'est pas interdit par le standard mais certains adaptateurs WiFi ne le gèrent pas correctement, ce qui peut poser des problèmes d'interopérabilité. C'est donc une solution à éviter.
- Un seul SSID peut être diffusé dans les trames balises. En revanche, l'AP répond aux requêtes de sondage (*probe requests*) pour tous les SSID qu'il gère. Ceci permet d'avoir un SSID visible et plusieurs SSID masqués. Cette solution est plus « interopérable » que la précédente mais est limitée à un seul SSID visible. En outre, ce type de produit utilise en général le même BSSID pour tous les SSID, ce qui n'est pas toujours bien géré par les adaptateurs WiFi : ils ont l'impression que l'AP change sans arrêt de SSID.
- L'AP peut émettre indépendamment des trames balise pour chaque SSID. Il y a alors deux options : certains AP utilisent le même BSSID pour chaque SSID (à éviter). En revanche, les meilleurs AP présentent un BSSID différent pour chaque SSID, ce qui donne réellement une illusion parfaite aux stations : tout se passe comme si plusieurs AP différents étaient présents (on parle d'AP virtuels). D'autre part, chaque service peut être différencié (avoir sa propre méthode d'authentification, sa propre sécurité, sa propre QoS...) : cette solution est donc nettement préférable aux précédentes.
- Pour finir, l'AP peut avoir plusieurs adaptateurs WiFi (ou plusieurs circuits radio), ce qui permet d'offrir plusieurs SSID, éventuellement même sur des canaux différents ! Cela revient techniquement à avoir plusieurs AP, mais on économise sur le matériel, le déploiement et la gestion.

Les AP multi-SSID permettent d'obtenir plusieurs réseaux sans fil distincts en ne déployant qu'une seule infrastructure.

Les paramètres qui peuvent être configurés pour chaque SSID dépendent du produit choisi. Certains AP permettent de choisir le nombre maximum de stations qui peuvent s'associer en même temps à un SSID, ou bien de choisir la radio utilisée (802.11a ou 802.11g par exemple) pour les AP à radios multiples. Certains permettent de modifier quelques aspects de la qualité de service (QoS) comme le débit maximal autorisé sur chaque réseau sans fil, ou enfin de changer le modèle de sécurité employé (WEP, 802.1x, WPA...). Certains AP sont munis de plusieurs ports LAN et il est possible d'associer un port LAN différent à chaque SSID. De cette façon, l'utilisateur peut se connecter à des réseaux filaires distincts selon le SSID sélectionné. Toutefois, la solution la plus fréquemment mise en œuvre pour gérer l'accès à des réseaux filaires multiples consiste à associer un SSID à un LAN virtuel (VLAN), comme nous allons le voir maintenant.

VLAN

Le concept de LAN virtuel est défini par l'IEEE dans la norme 802.1Q. Le but est de permettre à plusieurs réseaux indépendants d'être déployés sur une même infrastructure physique. Pour cela, un nouveau champ est rajouté dans chaque paquet : l'identifiant du VLAN (ou VLAN ID). Il s'agit d'un simple nombre codé sur 12 bits, ce qui permet de distinguer les paquets appartenant à différents réseaux virtuels (jusqu'à 2^{12} = 4 096 réseaux distincts) sur une même infrastructure.

Les commutateurs jouent un rôle central dans cette architecture à VLAN multiples : ce sont eux qui acheminent chaque paquet en fonction du VLAN auquel il appartient. Ils doivent également savoir gérer les paquets « classiques » qui ne sont pas associés à un VLAN, soit en les rejetant, soit en les laissant passer tels quels, soit en les laissant passer après leur avoir rajouté un VLAN ID particulier : on dit alors que le commutateur marque (*tag*) les paquets. Enfin, ils doivent éliminer le VLAN ID de tous les paquets avant de les retransmettre vers des portions du réseau ne gérant pas le 802.1Q ; en particulier, vers les stations, car la plupart des adaptateurs réseau des stations ne gèrent pas le 802.1Q.

Le choix du VLAN auquel un paquet non marqué est associé dépend en général simplement du port sur lequel il est reçu. Par exemple, un commutateur Ethernet à 16 ports pourrait être configuré pour que les paquets non marqués arrivant sur les ports 1 à 4 soient associés au VLAN n° 1. Les ports 5 à 8 pourraient être associés au VLAN n° 2. Sur les ports 9 à 16, le commutateur pourrait simplement éliminer les paquets non marqués. Certains commutateurs utilisent d'autres règles pour marquer les paquets : l'adresse MAC de la station source du paquet, ou encore le type de protocole de couche 3 (ou supérieur) qui est véhiculé par le paquet. Dans le cas d'un AP multi-SSID, les paquets peuvent également être marqués en fonction du SSID sélectionné.

Dans des bureaux occupés par des entreprises différentes, les VLAN sont particulièrement intéressants : toutes les stations sont reliées à une même infrastructure réseau par l'intermédiaire de commutateurs 802.1Q et ces commutateurs sont configurés pour marquer les paquets avec un VLAN différent pour chaque entreprise. De cette façon, une simple reconfiguration des commutateurs est suffisante lors des réaménagements

de bureaux. Bien qu'elles utilisent le même réseau physique, chaque entreprise ne verra que son propre trafic réseau.

Les VLAN peuvent également être utilisés au sein d'une même entreprise, par exemple pour avoir un réseau distinct pour chaque service (comptabilité, direction, R&D...). Les avantages d'une telle séparation des réseaux sont nombreux :

- coût d'infrastructure réduit ;
- sécurité importante si les VLAN sont bien isolés[1] ;
- facilité de maintenance car il n'y a qu'une seule infrastructure physique à gérer et que les éventuels problèmes sur un VLAN ne se répercutent pas sur les autres VLAN ;
- optimisation de la bande passante car le trafic broadcast n'est pas diffusé entre VLAN différents.

Les AP multi-SSID et multi-VLAN offrent précisément les mêmes avantages pour les réseaux sans fil : il est possible de déployer une seule et même infrastructure WiFi dans tout un bâtiment et d'y relier plusieurs entreprises ou plusieurs services distincts. Dans un contexte de *hotspot*, grâce aux VLAN, une même infrastructure peut être employée par plusieurs fournisseurs d'accès à Internet sans fil (*Wireless Internet Service Providers*, WISP).

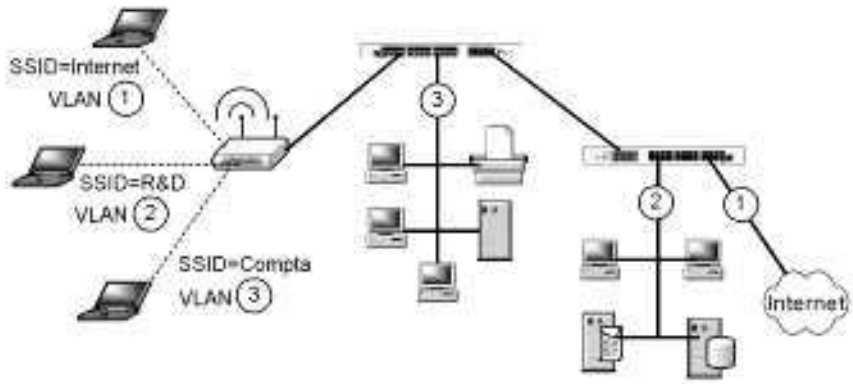


Figure 4.11 — Une architecture multi-SSID et multi-VLAN.

1. Attention : ceci peut varier d'un produit à l'autre. Certains commutateurs réagissent mal lorsqu'ils saturent : ils laissent tout à coup passer tous les paquets dans tous les VLAN ! Un pirate peut donc saturer volontairement le commutateur avec du trafic inutile, jusqu'à ce que le commutateur « craque ». Il a ensuite accès aux autres VLAN. Toutefois, les commutateurs VLAN récents sont en général très sûrs.

4.2.4 Le routeur

Les AP que nous avons décrits jusqu'à présent offrent une fonction d'AP ainsi que des services supplémentaires au niveau de la couche 2 du modèle OSI : pont, commutateur, STP, VLAN, etc. Il existe également des produits qui proposent, en supplément, des services au niveau de couches supérieures et notamment la couche réseau (niveau 3 dans le modèle OSI).

C'est à ce niveau que l'on trouve les *routeurs* WiFi. Un routeur est un équipement réseau qui se situe à l'interface entre au moins deux réseaux ou sous-réseaux (*subnets*) distincts et qui se charge d'acheminer (de « router ») les paquets entre ces réseaux. On parle également de passerelle (*gateway*). La plupart des routeurs permettent de relier deux LAN, ou bien un LAN et un WAN (en général Internet). En entreprise, les routeurs reposent presque toujours sur le protocole IP, mais il existe des routeurs pour d'autres protocoles de la couche 3, par exemple : IPX, CLNP (ISO 8473), etc.

Qu'il repose sur le WiFi, l'Ethernet ou sur tout autre protocole de niveau 2, un routeur IP fonctionne toujours de la même manière : c'est le principe même de la séparation des protocoles en couches séparées. Il ne serait donc pas opportun de nous livrer ici à une description détaillée des réseaux IP, ou du fonctionnement d'un routeur. Nous supposerons donc que vous connaissez les réseaux IP et en particulier l'adressage IP, les règles de routage, le DHCP, le DNS, le NAT, l'ARP, l'ICMP, le TCP, l'UDP, le GRE, etc. Si vous avez besoin d'une « piqûre de rappel », n'hésitez pas à consulter sur le site *www.livrewifi.com* l'annexe A qui est prévue à cet effet.

Un routeur WiFi est un produit « 2 en 1 » : un AP et un routeur réunis dans un même boîtier. Il serait fonctionnellement équivalent de connecter un AP pont à un routeur IP classique. L'interface de configuration du routeur WiFi permet donc de paramétrer à la fois les fonctions classiques et plus ou moins perfectionnées d'un routeur (tables de routage, serveur DHCP, NAT statique, RIP...) et le port WLAN (SSID, canal, clés WEP...), comme pour tout AP.

Presque tous les produits de micro-informatique peuvent être regroupés en un seul produit, par soucis de simplicité ou pour réduire les coûts. Par exemple, vous avez sans doute déjà vu des imprimante/scanneur qui semblent bien pratiques. Pourtant, à part chez les particuliers ou dans de petites sociétés, on trouve d'un côté les imprimantes et de l'autre les scanneurs. De la même manière, les grosses sociétés préfèrent souvent acheter d'une part un pare-feu et d'autre part un routeur plutôt qu'un routeur/pare-feu. De même, la plupart des sociétés d'une certaine taille préfèrent acheter les AP et les routeurs indépendamment. Il y a deux raisons principales à cela :

1. Un routeur WiFi est souvent (quoique pas toujours) un routeur de qualité moyenne couplé à un AP de qualité moyenne. Pour trouver un excellent routeur ou un excellent AP, on a en général plus de choix dans les produits autonomes : puisqu'ils sont spécialisés dans une seule tâche, ils sont souvent de meilleure qualité et plus paramétrables.
2. On doit souvent déployer beaucoup plus d'AP que de routeurs : un rapport de 10 à 20 AP pour un routeur n'est pas rare. L'intérêt d'intégrer une fonction d'AP dans les routeurs est donc limité.

Toutefois, dans certains contextes, les routeurs WiFi peuvent être intéressants, car il y a moins de matériel à acheter, à installer, à configurer et à superviser. Les routeurs WiFi sont particulièrement appréciés dans les contextes suivants :

- réseau sans fil familial : les « *box* » des opérateurs ADSL en sont les parfaits exemple ;
- réseau sans fil d'une PME, dans le cas où un seul AP est suffisant pour couvrir l'ensemble des bureaux ;
- petits *hotspots* (voir paragraphes suivants, le *hotspot-in-a-box*).

4.2.5 Le hotspot et le contrôleur d'accès

Pourquoi les hotspots vous concernent

Rappelons qu'un *hotspot* est un point d'accès public à Internet sans fil. Il peut également donner accès à d'autres services comme de la téléphonie, des jeux, des vidéos, etc. Vous pouvez légitimement vous demander en quoi les *hotspots* concernent votre entreprise. Voici trois réponses :

1. Votre entreprise peut souhaiter mettre en place un *hotspot* dans ses propres locaux afin de donner accès à Internet à ses visiteurs (clients, fournisseurs, prospects...). Les visiteurs peuvent apprécier ce service et cela peut augmenter la productivité des réunions : les visiteurs peuvent faire des démonstrations directement sur Internet, par exemple. Cela permet également d'éviter de connecter à votre réseau privé des personnes étrangères à votre société, pour des raisons de sécurité.
2. Même si vous ne souhaitez pas installer de *hotspot* dans votre entreprise, vos employés seront susceptibles de les utiliser pendant leurs déplacements. Ceci peut également représenter un gain de productivité, en particulier pour les commerciaux qui sont souvent en déplacement. Certains fournisseurs d'accès à Internet sans fil (WISP) proposent des abonnements groupés pour entreprises.
3. Il est important de savoir comment fonctionnent les *hotspots* et surtout quelles sont leurs failles de sécurité, car vos employés s'y connecteront sans doute avec leur ordinateur portable d'entreprise ! Des documents confidentiels peuvent alors être compromis.

Le cahier des charges

Dans les *hotspots*, le mot d'ordre est l'accessibilité, c'est-à-dire la simplicité de connexion : il faut que toute personne équipée d'un adaptateur WiFi puisse se connecter facilement, sans avoir besoin d'installer un logiciel particulier et quelle que soit sa configuration réseau (idéalement).

Les personnes qui ne sont pas encore abonnées au service doivent pouvoir s'inscrire facilement *via* le *hotspot*, mais ne doivent avoir accès qu'à un service limité, par exemple l'accès à une liste restreinte de sites web, appelée la *white-list* (liste blanche).

L'accès à Internet ou à tout autre service doit être contrôlé et peut être payant. Le volume de données téléchargées ou le temps passé sur Internet peuvent servir à la

facturation, qui peut être prépayée (avec des coupons de connexion) ou post-payée (par un abonnement). Toutes les transactions doivent être aussi sécurisées que possible.

Les contrôleurs d'accès pour *hotspots* ont été conçus afin de répondre à ce cahier des charges. Il s'agit souvent de serveurs dédiés à cette unique tâche, placés entre les AP et les services (en général l'accès à Internet) : le contrôleur d'accès est un point de passage obligatoire, comme le péage à l'entrée d'une autoroute. Il a en général des fonctions de routeur et de pare-feu (*firewall*), ainsi que des fonctions d'identification et de contrôle des connexions des utilisateurs.

Un contrôleur d'accès peut également être intégré dans un AP. Un tel AP + contrôleur d'accès est souvent appelé un *hotspot-in-a-box* (*hotspot*-dans-une-boîte) car un seul boîtier permet alors de mettre en œuvre un *hotspot* : il permet d'économiser un ordinateur dédié en offrant à la fois la fonction d'AP et la fonction de contrôleur d'accès (fig. 4.12).

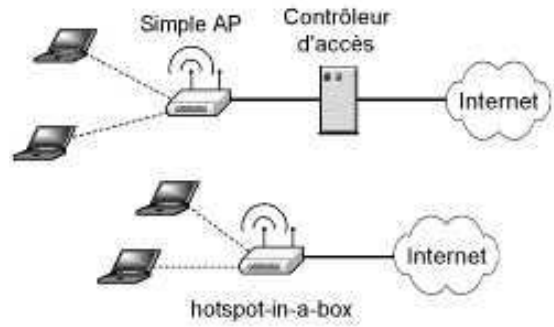


Figure 4.12 — Deux architectures typiques pour un petit *hotspot*.

Un réseau sans fil ouvert

Regardons les points du cahier des charges et voyons ce qu'ils impliquent. Tout d'abord, pour permettre à tout le monde d'accéder facilement au service, il doit y avoir un SSID visible. Ensuite, il est malheureusement nécessaire que le réseau sans fil correspondant à ce SSID ne soit pas sécurisé : en effet, le WEP, le 802.1x, le WPA et le WPA2 supposent tous un minimum de configuration qui n'est pas forcément à la portée du premier venu. Ceci est d'autant plus important qu'il est nécessaire d'accepter les visiteurs non abonnés pour qu'ils puissent s'inscrire. Avec un SSID visible et un réseau sans fil non sécurisé, n'importe qui peut s'associer facilement. Une fois associé, le client doit recevoir automatiquement sa configuration IP par DHCP : le contrôleur d'accès doit être serveur DHCP. Par la suite, le contrôleur d'accès repère les clients non identifiés, en général par le biais de leur adresse MAC et il leur interdit l'accès à certains services, en filtrant leur trafic réseau à la manière d'un pare-feu.

Pour que les nouveaux venus puissent s'inscrire et que les abonnés puissent s'identifier, la solution la plus courante consiste à ce que le contrôleur d'accès redirige tout le trafic web (sauf la *white-list*) vers une page web d'accueil, on parle de « portail

captif ». Cela signifie qu'une fois associé au réseau WiFi, le client n'a plus qu'à démarrer son navigateur Internet pour parvenir à la page d'accueil du WISP. Le visiteur sans abonnement peut s'inscrire ou saisir l'identifiant d'un coupon de connexion prépayé qu'il aurait acheté sur site et l'abonné qui possède déjà un compte crédité peut simplement s'identifier au travers d'un formulaire sur une page web. Le contrôleur d'accès peut alors vérifier les identifiants du client (éventuellement en consultant un serveur d'identification). Après cette étape, le contrôleur d'accès laisse passer le client vers les services auxquels il a droit.

L'identification des utilisateurs

Le contrôleur d'accès le plus simple est un *hotspot-in-a-box* relié à une petite imprimante de tickets. Lorsqu'un client demande à se connecter, le propriétaire du *hotspot* lui imprime un coupon de connexion qui contient un identifiant et un mot de passe valables pendant un certain temps. Il demande également au client de payer, comme on paierait une boisson. Ce *hotspot-in-a-box* est complètement autonome et ne suppose même pas de WISP. En contrepartie, le service est limité : le propriétaire du site doit intervenir pour chaque client, il n'y a pas de paiement en ligne par CB, pas de *roaming* possible, pas de hotline, pas d'abonnement... bref, c'est une solution pratique, mais pour un petit *hotspot* tel qu'un café. Certaines entreprises optent pour cette solution pour offrir un accès Internet à leurs visiteurs et la procédure d'impression de coupon pour chaque client impose une vérification de l'identité des utilisateurs qui n'est pas pour déplaire à la direction informatique, soucieuse de ne pas laisser des inconnus utiliser ses ressources.

Une solution plus perfectionnée et plus fréquente, consiste à utiliser un contrôleur d'accès capable de vérifier les identifiants des utilisateurs auprès d'un serveur centralisé. Les deux principaux protocoles utilisés sont :

- *Lightweight Directory Access Protocol* (LDAP) ;
- *Remote Authentication Dial In User Service* (RADIUS).

La solution LDAP

LDAP est un protocole très répandu qui permet de consulter des annuaires (un carnet d'adresse, par exemple). Il définit à la fois comment un annuaire doit être structuré, le type d'information qu'il doit contenir, comment les entrées qu'il contient doivent être nommées, comment on peut accéder à ces informations, le protocole pour le faire (se connecter à un annuaire, se déconnecter, rechercher, comparer, créer, effacer ou modifier des entrées), comment sécuriser les échanges et même comment les informations peuvent être réparties entre plusieurs serveurs. Un annuaire est comparable à une base de données, mais il est optimisé pour être consulté beaucoup plus souvent qu'il n'est modifié et il ne requiert pas de cohérence absolue. Par exemple, sur un annuaire distribué sur plusieurs serveurs, si une entrée est modifiée sur un serveur, il n'est pas garanti que les autres serveurs seront synchronisés immédiatement.

Un annuaire LDAP est bien adapté pour stocker des identifiants et leur mot de passe et nombreuses sont les sociétés qui enregistrent dans un annuaire LDAP

ces informations pour tous leurs employés. Des logiciels d'e-mails tels que Microsoft Outlook sont capables de consulter un annuaire LDAP pour obtenir l'adresse e-mail et toute autre information sur un contact. Pour un contrôleur d'accès, un serveur LDAP peut servir à centraliser les identifiants et mots de passe des utilisateurs. Mais on a souvent besoin de bien plus d'informations : la durée maximale de la connexion de l'utilisateur, les services auxquels il a droit, etc. En outre, on peut vouloir stocker des informations telles que la durée de la session, le volume des données téléchargées ou envoyées, etc. Pour cela, le service LDAP est insuffisant et la solution RADIUS est bien plus adaptée.

La solution RADIUS

Le protocole RADIUS a été conçu pour permettre à un équipement contrôlant l'accès à un réseau, qu'on appelle un *Network Access Server* (NAS), de pouvoir communiquer avec un serveur centralisé, le « serveur RADIUS », afin de :

- vérifier l'identité d'un utilisateur qui cherche à se connecter ;
- savoir quels sont ses droits d'accès et sa configuration particulière ;
- comptabiliser les connexions, leur durée, le volume de données échangées et tout autre paramètre de connexion pouvant servir à la facturation du client ou à son suivi.

Dans notre cas le NAS correspond simplement au contrôleur d'accès, inclus dans le *hotspot-in-a-box*. Nous approfondirons le protocole RADIUS au chapitre 10.

Transparence SMTP

Afin de rendre la connexion à un *hotspot* aussi simple que possible, les contrôleurs d'accès WiFi peuvent mettre en œuvre quelques fonctions avancées qui permettent aux utilisateurs de profiter de leur connexion sans avoir à reconfigurer leur ordinateur portable ou PDA. La première de ces fonctions est la transparence SMTP.

Voyons au travers d'un exemple les problèmes que l'on peut rencontrer sur un *hotspot* qui ne met pas en œuvre de transparence SMTP : Sophie possède, chez elle, un abonnement à un FAI donné (par exemple, Wanadoo). Elle a donc configuré son logiciel d'e-mail pour utiliser le serveur SMTP de son FAI : smtp.wanadoo.fr. Un jour, elle se connecte à un *hotspot* avec son ordinateur portable. Ce *hotspot* est mis en œuvre par un autre FAI, mettons Oreka, donc Sophie doit créer un compte chez Oreka et s'identifier, par exemple en saisissant son numéro de téléphone portable auquel un SMS[1] est envoyé, contenant un code d'activation. Lorsque Sophie essaie d'envoyer un e-mail avec son logiciel habituel, celui-ci tente d'établir une connexion avec le

1. Un *Short Message Service*, ou « texto », est un bref message envoyé à une personne sur son téléphone portable. Une autre méthode d'identification du client consiste à lui demander son adresse e-mail et à envoyer un code d'activation du compte à cette adresse. Certains FAI suivent une procédure plus longue mais plus sûre pour identifier leur client (envoyer une lettre avec son adresse de courrier « physique »).

serveur smtp.wanadoo.fr. Malheureusement, pour des raisons de sécurité[1], le serveur SMTP de Wanadoo refusera la requête, car Sophie se connecte au travers d'un autre FAI.

Une solution pour Sophie serait de reconfigurer son logiciel d'e-mail pour remplacer smtp.wanadoo.fr par smtp.oreka.fr, mais ce serait assez pénible et elle devrait refaire la manipulation inverse en rentrant chez elle. C'est ici que la transparence SMTP intervient : le contrôleur d'accès peut intercepter tout trafic de type SMTP et le rediriger vers smtp.oreka.fr. De cette façon, Sophie pourra envoyer des e-mails sans avoir à reconfigurer quoi que ce soit. Il existe toutefois des cas où la transparence SMTP ne fonctionne pas : en particulier, si Sophie a activé dans son logiciel d'e-mail l'authentification SMTP (en supposant que son serveur Wanadoo le permette), alors Sophie peut envoyer des e-mails en utilisant ce serveur Wanadoo, quel que soit le FAI par lequel elle passe pour accéder à Internet. Dans ce cas, la transparence SMTP doit absolument être désactivée, sinon le serveur Oreka recevra une demande d'authentification destinée à Wanadoo, ce qui donnera vraisemblablement une erreur.

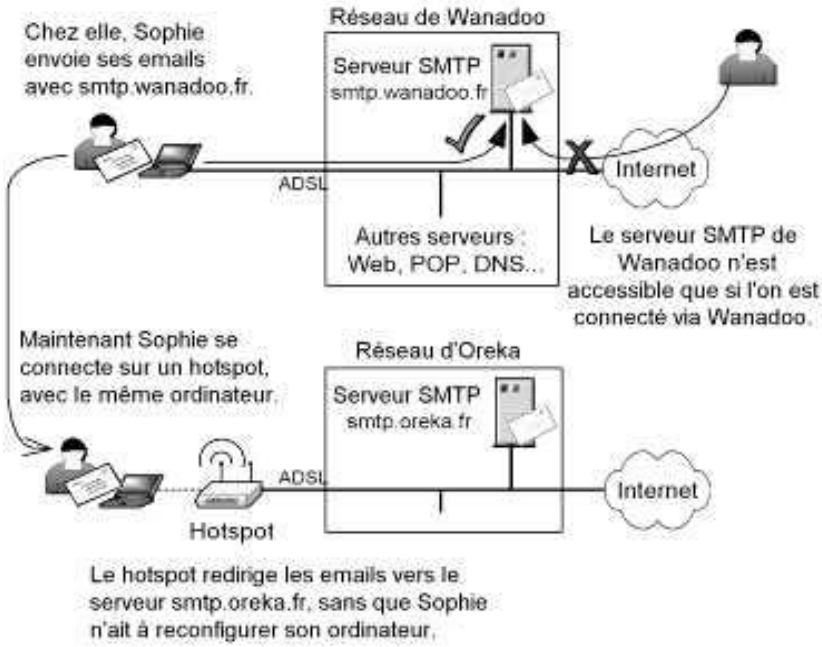


Figure 4.13 — L'intérêt de la transparence SMTP.

1. Pour éviter que des inconnus puissent envoyer des milliers de messages non sollicités (le *spam*).

Transparence proxy

Dans de nombreuses sociétés, les navigateurs Internet des employés sont configurés pour accéder au Web en passant par un « serveur proxy[1] ». Celui-ci a pour but d'optimiser l'accès à Internet en stockant localement les pages web les plus fréquemment visitées. Voyons pourquoi cela pose un problème dans les *hotspots*.

Admettons que Patrice travaille dans une société qui a mis en œuvre un serveur proxy à l'adresse 10.0.0.120. Le navigateur web de Patrice doit être configuré pour utiliser ce serveur proxy. Si Patrice se connecte à un *hotspot* et qu'il démarre son navigateur Internet, celui-ci cherchera le serveur proxy mais ne pourra pas le trouver, car le serveur proxy est local à l'entreprise de Patrice. Pour résoudre le problème, Patrice peut aller dans ses paramètres Internet et supprimer la configuration du proxy. Mais il n'aura peut-être pas les droits pour le faire car certaines sociétés figent la configuration réseau des postes de leurs employés. D'autre part, même s'il peut le faire, il faudra qu'il y pense, ce sera pénible et il devra refaire le changement au retour dans sa société.

Les contrôleurs d'accès qui mettent en œuvre la transparence proxy interceptent tout le trafic adressé à un serveur proxy et agissent comme s'ils étaient eux-mêmes le proxy. De cette façon le client peut se connecter sans difficulté et sans reconfigurer son poste.

Introduction au 802.1x

Comme nous l'avons vu, dans le contrôleur d'accès d'un *hotspot*, le souci de simplicité absolue de configuration a poussé les WISP à mettre en œuvre un mécanisme qui ne suppose aucune installation de logiciel ou configuration sur le poste du client : l'interface de connexion du client est son navigateur Internet, le protocole de communication entre le client et le NAS est HTTPS (ou HTTP, si le *hotspot* n'est pas du tout sécurisé !). L'inconvénient de cette méthode est qu'elle se déroule au niveau d'une couche réseau bien supérieure au WiFi. La conséquence est que l'on doit autoriser tous les clients à s'associer au niveau WiFi, leur attribuer une adresse IP et leur donner accès à une partie du réseau (au moins jusqu'au contrôleur d'accès) avant de décider s'ils ont le droit d'utiliser le service ou non ! Ce n'est pas très logique et cela laisse plus de marge aux pirates pour tester les limites de sécurité du système. En particulier, si les AP n'interdisent pas aux clients de se voir entre eux, un pirate peut déjà attaquer les autres clients connectés sans fil ! En outre, l'interface client n'est pas standardisée et chaque WISP peut proposer sa méthode de connexion.

Il existe une méthode de contrôle d'accès standard plus flexible que la méthode HTTPS : il s'agit du protocole 802.1x que nous approfondirons dans le chapitre 8. Le 802.1x est mis en œuvre par chaque point d'accès pour identifier les clients : chaque AP sert alors de NAS. Le protocole 802.1x se déroule directement sur la couche MAC, de sorte que tout le processus peut avoir lieu juste après l'association (qui est libre), mais avant que le client ne reçoive une adresse IP ou puisse accéder au réseau.

1. *by proxy* signifie « par procuration ». Un *proxy* est un intermédiaire.

Les principaux systèmes d'exploitation gèrent désormais bien le 802.1x, mais il reste malheureusement un peu technique à utiliser. Ainsi, afin de conserver une grande facilité de connexion pour tous les visiteurs d'un *hotspot* tout en offrant un niveau de sécurité important aux abonnés qui le souhaitent, certains *hotspots* mettent en œuvre plusieurs SSID, l'un reposant sur la solution classique avec HTTPS (le portail captif) et l'autre sur WPA, qui repose lui-même sur le 802.1x, comme nous le verrons au chapitre 9.

Toutes sortes d'autres fonctions avancées peuvent être intégrées dans un contrôleur d'accès, mais nous avons présenté les fonctions principales d'un *hotspot* :

- SSID visible et réseau sans fil non sécurisé pour faciliter la connexion ;
- transparence SMTP et proxy, également pour faciliter la connexion ;
- redirection des clients non identifiés vers une page d'accueil ;
- identification des clients, souvent par l'intermédiaire d'un serveur RADIUS ;
- contrôle de la connexion du client (sites interdits, temps limité...) ;
- un deuxième SSID sécurisé par WPA, pour les clients soucieux de sécurité.

4.2.6 La configuration d'un AP

Qu'il s'agisse de simples ponts, de routeurs ou de *hotspot-in-a-box*, les AP proposent en général une interface d'administration (fig. 4.14). La procédure exacte d'accès à l'interface d'administration, la configuration IP nécessaire et les identifiants « administrateur » par défaut pouvant varier d'un produit à un autre, il faut consulter la documentation de l'AP.

L'interface d'administration elle-même est en général une interface web, ou parfois une interface Telnet (en ligne de commande). Il peut également arriver qu'il soit nécessaire d'installer un logiciel d'administration fourni pas le constructeur. Quoi qu'il en soit, vérifiez que l'interface soit assez intuitive et complète.

Certains AP peuvent télécharger automatiquement leur configuration par FTP, HTTP ou encore RADIUS. Ceci peut être pratique si le nombre d'AP est important, car on peut alors centraliser et homogénéiser la configuration du parc. Une autre fonction intéressante est la possibilité d'exporter la configuration dans un fichier pour pouvoir la recharger ultérieurement.

4.2.7 Comment choisir un AP ?

Pour conclure et résumer cette section dédiée aux AP, voici une liste de questions à se poser (ou à poser au vendeur) avant l'achat d'un AP.

Couche physique

Comme pour tous les produits WiFi, le premier critère de choix d'un AP est la norme utilisée : 802.11a, 802.11b, 802.11g ou encore des AP mixtes (802.11a/g) voire propriétaires (802.11b+...).

Figure 4.14 — Exemple d'interface web d'administration d'un point d'accès.

Observez attentivement les caractéristiques radio de l'AP : puissance de l'émetteur, gain de l'antenne, profil de radiation de l'antenne (angle horizontal et vertical de rayonnement de l'antenne), sensibilité, tolérance au bruit, modulations gérées, etc. *Attention* : tout le monde se focalise sur la portée, mais il ne s'agit pas forcément du critère le plus important en entreprise. En effet, si vous avez 500 employés dans votre entreprise et que vous installez un AP extraordinaire capable de couvrir tout le bâtiment et de gérer 500 connexions simultanées, le débit moyen par utilisateur sera ridicule car les 11 Mb/s ou 54 Mb/s disponibles seront partagés en 500. Il est donc souvent préférable de déployer beaucoup d'AP de faible portée. Nous verrons au chapitre 5 comment optimiser les paramètres radio selon le contexte.

> En entreprise, la portée des AP n'est pas forcément le critère le plus important, car il faudra sans doute déployer de nombreux AP pour pouvoir gérer de multiples connexions simultanées.

Couche MAC

Soyez attentif aux fonctionnalités de la couche 2. Voici quelques questions à se poser :

- Quel niveau de sécurité est géré ? Le WPA ou le WPA2, ce qui serait idéal ? Est-il possible d'isoler les stations associées pour qu'elles ne se voient pas ?
- Le PCF est-il pris en charge ? Ou mieux, le WMM ? L'interface de configuration permet-elle de régler finement la qualité de service (QoS), en particulier pour

attribuer équitablement la bande passante aux utilisateurs, offrir des priorités variables aux différents types de trafic réseau (Web, e-mails, multimédia...) ?

- Peut-on avoir plusieurs SSID ? Chaque SSID a-t-il alors son propre BSSID ? Peut-on rendre plusieurs SSID visibles ? Chaque SSID peut-il être associé à un ou plusieurs VLAN ? Chaque SSID peut-il avoir sa propre configuration de sécurité ?
- Combien y a-t-il de ports LAN ? Peut-on chaîner les AP *via* leurs ports LAN ?
- Le WDS est-il pris en charge ? Avec quel algorithme de routage ? Y a-t-il un algorithme de routage propriétaire ?
- Le STP est-il géré ?
- L'interface de configuration permet-elle de régler de nombreux paramètres de la couche MAC, tels que le RTS *Threshold* ou le seuil de fragmentation (voir le chapitre 3) ?

Services de couches supérieures

S'il s'agit d'un routeur WiFi, quelles sont les fonctions offertes ? Y a-t-il un pare-feu ? Sa configuration est-elle facile ? Les règles de routage peuvent-elles être modifiées ? Le routeur gère-t-il le NAT dynamique ? Le NAT statique ? Peut-il être serveur DHCP ? Gère-t-il d'autres services de couche 3 (RIP, IGMP, IPX...) ? Bref, choisissez-le comme un routeur classique et n'oubliez pas que vous pouvez très bien acheter indépendamment un routeur classique et un AP.

S'il s'agit d'un *hotspot-in-a-box*, soyez particulièrement attentif à la méthode d'authentification utilisée : est-ce une simple génération de coupons de connexion imprimés ou bien le contrôleur d'accès repose-t-il sur LDAP, RADIUS ou autre ? Quel est le niveau de sécurité offert pour protéger les identifiants échangés : HTTP ou HTTPS ? Gère-t-il une *white-list* ? Une *black-list* ?

Administration et supervision

Pour finir, l'interface d'administration de l'AP est-elle ergonomique et complète ? Tous les paramètres sont-ils faciles à configurer ? Est-ce une interface web ou Telnet ou autre ? Est-il possible de mettre à jour le *firmware* de l'AP ? Gratuitement ? Les mises à jour sont-elles fréquentes et de qualité ? Dans quelle mesure l'AP sera-t-il capable d'être mis à jour pour suivre les évolutions des normes de sécurité et de QoS ? L'AP peut-il télécharger sa configuration tout seul ? Offre-t-il une interface de supervision ? Par SNMP ?

Autres critères de choix

Bien entendu, la marque du constructeur est un critère de choix essentiel. La fiabilité et la réactivité varient naturellement d'un fournisseur à l'autre : c'est à vous de vous faire une idée du marché et de ses acteurs. Les groupes de discussions et les retours d'utilisateurs peuvent vous donner des indications précieuses pour le choix d'un fournisseur et d'un produit en particulier.

Le format de l'AP est tout aussi important : l'ergonomie, la résistance aux chocs, à la température, à l'humidité sont autant de critères à prendre en compte, selon le contexte du déploiement. Dans un lieu peu surveillé, faites attention à choisir un AP que vous pourrez visser à un mur, voire dans un faux plafond. Certains AP ont une antenne ou un adaptateur WiFi détachable, ce qui est très pratique lorsque l'on souhaite mettre à jour son matériel ou changer la couverture radio, mais il faut faire attention à ce que ces composants ne soient pas volés !

La consommation électrique peut être un critère non négligeable lorsque vous déployez plusieurs dizaines d'AP. Enfin, assurez-vous que les composants ne se déconnectent pas trop facilement tout seuls, en particulier l'alimentation électrique, l'adaptateur WiFi et l'antenne.

4.3 LES PÉRIPHÉRIQUES WIFI

Dans cette section, nous allons présenter très brièvement les principaux types de périphériques WiFi que l'on peut trouver en magasin. Ils sont trop nombreux pour que nous puissions entrer dans les détails, mais une présentation d'ensemble vous donnera peut-être des idées d'applications auxquelles vous n'aviez pas pensé ?

4.3.1 Les périphériques de bureautique

Ordinateurs, Tablet PC, PDA et smartphones

Les premiers périphériques WiFi sont bien sûr les ordinateurs de bureau et les ordinateurs portables, dont certains sont vendus avec un adaptateur WiFi intégré. Viennent ensuite les Tablet PC, les PDA (Palm, Pocket PC) et les smartphones, très pratiques pour des usages réellement mobiles, comme des inventaires sans fil ou simplement des audits radio. Pour des raisons de taille et de consommation électrique, les adaptateurs WiFi des PDA sont souvent limités à une seule radio (2,4 GHz ou 5 GHz) peu puissante, donc il est important de bien vérifier les caractéristiques WiFi selon l'application visée.

Les Tablet PC offrent un compromis entre les PDA et les ordinateurs portables et sont intéressants pour des applications qui requièrent à la fois puissance et mobilité.

Figure 4.15 — Quelques produits avec le WiFi intégré.

Imprimantes

Les imprimantes WiFi sont pratiques dans un contexte familial ou dans une PME, surtout s'il n'y a pas de réseau filaire ! Toutefois, dans les entreprises plus grandes, ces périphériques sont souvent assez volumineux et sont rarement amenés à être déplacés. Du coup, si la société dispose d'un réseau filaire, l'intérêt de connecter les imprimantes en WiFi est très limité et consomme de la bande passante sur le réseau sans fil pour rien. En entreprise, à moins que le contexte n'impose le WiFi, on préférera en général les imprimantes « classiques ».

On peut également connecter une imprimante classique à un serveur d'impression WiFi : il s'agit d'un petit boîtier WiFi doté d'un connecteur d'imprimante. Plusieurs postes peuvent ainsi utiliser une même imprimante classique au travers du WiFi, même si cette imprimante n'a pas été conçue pour être utilisée en réseau. À nouveau, ces produits ne sont réellement utiles que chez soi, en PME, ou bien lorsque l'imprimante ne peut pas physiquement être branchée au réseau filaire.

Vidéoprojecteurs

Les vidéoprojecteurs WiFi sont particulièrement pratiques : ils permettent de réaliser des présentations sans avoir à connecter son ordinateur portable avec un câble au vidéoprojecteur. Les présentations peuvent être plus vivantes et interactives car l'animateur peut se déplacer avec son ordinateur portable pendant la présentation, au gré des discussions. Ils permettent également à plusieurs personnes de faire des présentations successives ou même simultanées. Malheureusement, ils supposent l'installation d'un logiciel sur le poste du client. En outre, ils sont assez gourmands en bande passante et ne permettent pas de projeter des animations de façon très fluide (telles qu'un DVD par exemple).

À nouveau, comme pour les imprimantes, il existe également des boîtiers qui se connectent au port d'entrée « standard » (VGA) d'un vidéoprojecteur quelconque. Ceux-ci ont l'intérêt de vous permettre de conserver votre vidéoprojecteur actuel ou bien d'en choisir un strictement pour ses qualités d'image et non pour sa connectivité.

Caméras

Les caméras de surveillance connectées en WiFi sont pratiques à déployer et sont parmi les périphériques WiFi les plus appréciés. L'usage de la bande passante peut être important, selon la qualité de l'image et la fréquence des prises de vue : il faut faire attention à ce que cela ne perturbe pas les autres utilisateurs du réseau sans fil, s'il y en a. En outre, ces caméras peuvent être gênées par des interférences (éventuellement volontaires), ce qui diminue le niveau de sécurité qu'elles offrent. Certaines caméras WiFi peuvent être reliées à un système de sécurité tiers (détection des mouvements, variations magnétiques, infrarouges...) et ne s'activer qu'en cas d'intrusion. Certains produits offrent la possibilité d'envoyer un e-mail pour prévenir le propriétaire en cas d'intrusion.

Multimédia

Pour finir, il existe de nombreux produits multimédias reposant sur le WiFi : des chaînes Hi-Fi équipées d'un adaptateur WiFi et capables de jouer des MP3 envoyés par votre ordinateur, des adaptateurs audio à connecter à une chaîne Hi-Fi classique, des écrans de télévision pouvant recevoir un flux vidéo envoyé par votre ordinateur ou encore une fois des adaptateurs vidéo WiFi à connecter à votre écran. L'intérêt de ces produits pour une entreprise semble limité, sauf peut-être pour orner la salle d'attente, mais ils ont un certain succès chez les particuliers.

Les photos de vacances, les vidéos de famille et tous ces souvenirs que l'on rangeait autrefois dans une vieille boîte à chaussure seront de plus en plus dématérialisés : stockés dans notre ordinateur, nos souvenirs seront transférés vers notre écran de télévision ou notre chaîne Hi-Fi grâce aux technologies sans fil telles que le WiFi. L'ordinateur devient notre boîte à chaussure digitale (*digital shoe box*).

4.3.2 Les outils d'analyse

Analyseurs complets

Les analyseurs sont en général des logiciels à installer sur un ordinateur portable (ou un PDA) tout à fait quelconque mais équipé d'un adaptateur WiFi compatible avec le logiciel choisi. Dans certains cas, l'adaptateur est un boîtier conçu spécialement pour le logiciel en question, mais le plus souvent il s'agit simplement d'une carte WiFi ordinaire, en mode *monitor* (pour pouvoir « sniffer » les paquets qui ne sont pas adressés à cet ordinateur).

Par exemple, le logiciel NetStumbler peut être téléchargé gratuitement et installé sur votre ordinateur portable. Si vous avez l'une des cartes WiFi recommandées par le logiciel, par exemple la carte PCMCIA Orinoco Gold de Proxim, alors votre ordinateur peut devenir un véritable outil d'analyse WiFi. Vous pouvez détecter tous les AP à proximité, les SSID qu'ils émettent, leurs adresses MAC, la puissance de réception et le rapport signal/bruit (RSB) pour chacun d'entre eux, ainsi que l'évolution de ces paramètres au cours du temps. Si en plus vous branchez l'un des modules de positionnement par satellite *Global Positioning System* (GPS) gérés par ce logiciel, vous pouvez vous promener sur le site à analyser (pourvu que vous captiez

le signal GPS), les enregistrements seront automatiquement localisés et les résultats tracés sur une carte de votre choix !

Il existe également des offres intégrées contenant un PDA, un adaptateur WiFi et un logiciel analyseur. C'est le cas par exemple du *YellowJacket* de Berkeley Varitronics Systems (BVS) ou encore du *Handheld* d'Airmagnet (fig. 4.16).

Figure 4.16 — Analyseurs et sondes.

Par ailleurs, certains AP intègrent des fonctions d'analyse, permettant par exemple de détecter les AP voisins ou de mesurer les interférences. Ces analyses peuvent ensuite être consultées *via* l'interface d'administration de l'AP (une interface web, le plus souvent) ou *via* une interface de supervision (en général sur SNMP).

Pour finir, certains de ces AP sont complètement dédiés à la tâche d'analyse : c'est le cas par exemple du *Sensor* d'Airmagnet dont la seule fonction est d'analyser le réseau sans fil à proximité de lui, passivement (en écoutant les ondes radio) ou activement (en essayant de se connecter aux AP voisins, par exemple). L'intérêt de ce modèle est que l'on peut installer une sonde pour tous les quatre à six AP « normaux », puis utiliser un logiciel de supervision centralisé pour surveiller le réseau sans fil en permanence. En cas de problème, par exemple si un réseau sans fil pirate est installé, alors une alarme, telle qu'un e-mail ou un SMS, peut être envoyée automatiquement.

Simples détecteurs

Les détecteurs WiFi sont souvent bon marché et de petite taille (fig. 4.17), parfois destinés à être également utilisés comme porte-clés, ils permettent de savoir immédiatement que l'on arrive à proximité d'un réseau WiFi, qu'il soit libre d'accès ou non.

En général, il suffit de pointer le détecteur dans une direction et d'appuyer sur un bouton pour détecter les réseaux présents : selon la puissance du signal reçu, un nombre plus ou moins important de lumières s'allument.

Les détecteurs permettent de ne pas perdre de temps à allumer son ordinateur portable pour se rendre compte qu'il n'y a pas de réseau sans fil disponible. Grâce au mécanisme de pointage, ils peuvent permettre de trouver très simplement la position des AP les plus proches.

Figure 4.17 — Quelques exemples de détecteurs WiFi.

4.3.3 Les périphériques « industriels »

Lecteurs sans fil

Des lecteurs WiFi de codes-barres, de cartes de crédit, ou d'autres systèmes spécialisés, sont utilisés dans l'industrie depuis quelques années. Les lecteurs de code-barres permettent par exemple d'enregistrer les bagages au moment de leur chargement dans un avion (comme nous l'avons vu au chapitre 1). Les passagers étant eux-mêmes enregistrés au moment de leur embarquement, les bagagistes peuvent savoir instantanément si le propriétaire d'un bagage particulier se trouve à bord ou non, ce qui est une contrainte de sécurité essentielle. De même, la question de la sécurité est centrale dans les lecteurs de cartes de crédit.

Pour ces applications, toute la sécurité offerte par le WiFi doit être déployée. Puisque le WiFi est une technologie standardisée et très répandue, les pirates ont naturellement plus de facilité à trouver du matériel, des outils et de la documentation pour détecter et attaquer les réseaux WiFi. Mais il ne faut pas oublier que le même argument est valable dans l'autre sens : de nombreux experts travaillent à rendre le WiFi plus sûr et les normes WPA et WPA2, éventuellement complétées par d'autres systèmes de sécurités (VPN, protocoles propriétaires...) garantissent un niveau de sécurité très élevé, adapté à ce type d'applications. En outre, rien n'empêche de compléter la sécurité du système avec d'autres algorithmes si nécessaire. Se tourner vers une technologie peu répandue en espérant que cela garantira la sécurité du système serait une erreur.

Outils de localisation

Les outils de localisation par le WiFi fonctionnent en général par triangulation : un logiciel installé sur le poste mobile WiFi (ordinateur portable ou PDA) détecte les AP situés à proximité et en fonction de la puissance du signal reçu de chacun d'eux, il en déduit la position de l'utilisateur. Cela suppose un étalonnage initial : par exemple, l'utilisateur fournit un plan du site au logiciel et lui indique où se trouvent les AP sur ce plan. Cet étalonnage initial permet par la suite au logiciel, pour la plupart des produits, de positionner l'utilisateur avec une précision d'environ deux mètres. Ce type de logiciel est pratique pour des audits de site, des inventaires sans fil et de nombreuses autres applications mobiles.

Plutôt que d'imposer l'installation d'un logiciel sur le poste mobile, il existe des AP dédiés à la localisation comme l'*AeroScout* de BlueSoft. Chaque station WiFi peut alors être localisée sans qu'un logiciel particulier ait besoin d'y être installé. Un logiciel

installé sur un serveur permet de savoir à tout instant où se trouvent les stations WiFi ! Ces AP de localisation peuvent mettre en œuvre des techniques de localisation plus précises, en supplément de la triangulation, par exemple en mesurant le décalage dans le temps de la réception du signal radio entre deux antennes attachées à l'AP.

En outre, de petits boîtiers peuvent être transportés par des personnes (le personnel de sécurité dans une entreprise, des enfants dans un parc d'attraction, les patients d'un hôpital...) ou installés sur des objets mobiles (véhicules dans un parking, caddies dans un supermarché, équipement médical dans un hôpital...). Ces outils de localisation peuvent servir à n'autoriser l'accès à une salle ou une machine qu'à condition que son responsable soit à proximité, par exemple. D'autres technologies sans fil sont parfois mieux adaptées que le WiFi pour cette fonction (voir le chapitre 1).

4.3.4 La téléphonie sur WiFi

Pour finir sur les périphériques WiFi, il faut signaler les téléphones WiFi, bien qu'ils ne soient pas encore très répandus. Leur principe est simple : ce sont des téléphones sans fil, tels que le *Wireless IP Phone* de Cisco ou encore le *WiFi vPhone* de Viper Networks, dont l'interface radio repose sur le WiFi, plutôt que sur d'autres technologies de téléphonie sans fil telles que le HomeRF, le GSM ou l'UMTS (voir le chapitre 1).

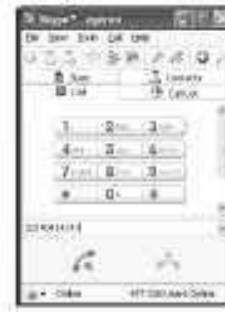
L'utilisateur doit d'abord sélectionner le réseau sans fil, en le choisissant dans la liste des réseaux détectés ou bien en saisissant manuellement le SSID et les paramètres du réseau WiFi. Par la suite, un protocole de voix sur IP (VoIP) tel que le protocole d'initiation de session (*Session Initiation Protocol*, SIP) est utilisé pour établir une communication avec un correspondant quelconque. Si ce correspondant utilise lui-même un téléphone sur IP, alors la communication passe simplement sur le réseau local ou sur Internet et la communication est donc gratuite. En revanche, si le correspondant possède un téléphone « classique » (mobile ou fixe), alors la communication devra transiter par une passerelle reliant l'Internet et le Réseau de téléphonie commutée (RTC). Pour pouvoir bénéficier de ces passerelles, il faut souscrire un abonnement auprès des sociétés qui les mettent en œuvre. Par la suite, pour chaque communication passant par une passerelle, le coût de la communication sera celui de la communication téléphonique entre la passerelle et le correspondant (plus la marge de la société, bien sûr). Puisque ces passerelles se situent un peu partout sur la planète, on ne paie en général que le prix d'une communication locale : le tarif est souvent bien inférieur à un appel classique dans une autre région de France !

De nombreuses sociétés s'intéressent donc à la VoIP pour diminuer le coût de leurs communications téléphoniques, surtout entre leurs succursales. C'est le cas en particulier des sociétés possédant des bureaux dans plusieurs pays. En déployant des téléphones sur IP dans tous ses bureaux, une société peut réduire considérablement sa facture téléphonique. Notons que ces téléphones sur IP ne doivent pas obligatoirement être WiFi : il peut s'agir de postes téléphoniques fixes, reliés directement au réseau filaire.

Des fonctions avancées telles que les boîtes vocales, les conférences téléphoniques, les annuaires ou encore les renvois d'appels sont gérés par des protocoles de VoIP

comme SIP ou le H.323, mais il faut en général installer un serveur de VoIP prévu à cet effet. Le H.323 permet même d'envisager des vidéoconférences.

Exemples de téléphones WiFi



L'interface de Skype

Figure 4.18 — La téléphonie sur WiFi : matériel ou logiciel.

Malheureusement, ces téléphones sur WiFi sont encore assez volumineux et leur autonomie est limitée (ceci est toutefois en train de changer). Une autre solution consiste à transformer un PDA ou un ordinateur portable (ou fixe) en téléphone sur WiFi. Pour cela, il suffit d'installer un logiciel prévu à cet effet, comme Skype, Wifive ou encore Net2Phone et de brancher un micro et une oreillette. Le résultat est certes moins pratique qu'un vrai téléphone, mais il est bien fonctionnel !

4.4 LES ANTENNES WIFI

Les antennes servent à la fois à l'émission et à la réception du signal électromagnétique : à l'émission, elles transforment en ondes électromagnétiques les signaux électriques générés par l'émetteur ; à la réception, elles transforment en courant électrique une onde électromagnétique émise par une autre antenne, de sorte qu'un récepteur pourra l'interpréter.

4.4.1 Comprendre les antennes

Le chapitre 5 traitera de la couverture radio et abordera en détail les règles de transmission radio. Pour l'heure, voici un bref aperçu des paramètres à prendre en compte pour l'achat d'une antenne.

Antennes actives ou passives

Les antennes se classent en deux catégories : les antennes passives et les antennes actives. Les antennes passives n'augmentent pas la puissance du signal, mais peuvent le concentrer dans une ou plusieurs directions. Les antennes actives peuvent également concentrer le signal mais elles contiennent, en plus, un amplificateur qui peut augmenter la puissance du signal reçu ou émis.

En France, étant donné que la réglementation interdit une puissance rayonnée supérieure à 10 ou 100 MW (2 ou 20 dBm) pour le 2,4 GHz, et 200 ou 1 000 mW (environ 23 dBm ou 30 dBm) pour le 5 GHz, les antennes actives à l'émission sont, de fait, interdites. L'amplification du signal reçu, n'est en revanche pas interdite, mais il faut alors une antenne de réception distincte de l'antenne d'émission.

En France, pour le WiFi, seules les antennes passives sont autorisées à l'émission : les antennes actives feraient dépasser la limite légale de puissance rayonnée.

Certains adaptateurs WiFi possèdent des emplacements pour connecter deux antennes : l'une uniquement pour la réception, l'autre à la fois pour la réception et l'émission. La première peut être active mais dans la pratique, les antennes passives sont bien suffisantes et moins chères, donc nous ne parlerons que de celles-ci. La présence de deux antennes en réception permet de mieux gérer les interférences en recevant le signal en double : c'est ce qu'on appelle la « diversité ». Pour cela, elles doivent être placées à une certaine distance l'une de l'autre, fonction de la longueur d'onde choisie.

La directivité

Une antenne peut rayonner de plusieurs façons, ce qui détermine sa catégorie :

- directionnelle, elle concentre le signal dans une direction donnée ;
- bidirectionnelle, elle concentre le signal dans deux directions (en général opposées) ;
- omnidirectionnelle (ou isotrope), elle ne concentre théoriquement pas du tout le signal et l'émet dans toutes les directions de l'espace, de façon homogène. Dans la pratique, de telles antennes n'existent pas. Le rayonnement n'est jamais homogène. Les antennes omnidirectionnelles concentrent en général le signal, non pas selon un axe, mais en l'aplatissant comme on écrase un ballon ;
- sectorielle, elle est à mi-chemin entre l'antenne directionnelle et l'antenne omnidirectionnelle en concentrant le signal dans une demi-sphère, ou un faisceau très large (par exemple de 60° d'angle).

En concentrant le signal dans l'espace, l'antenne directionnelle permet au récepteur (à condition qu'il soit dans l'axe bien sûr) de recevoir un signal d'une puissance plus importante que si l'antenne était parfaitement omnidirectionnelle. L'analogie classique de ce phénomène est celle de la lampe de poche : en réglant la lampe, vous pouvez concentrer plus ou moins son faisceau lumineux. Bien que la puissance de l'ampoule reste constante, une personne éclairée recevra plus de puissance lumineuse si le faisceau est concentré dans sa direction.

Le gain

Lorsqu'on est dans l'axe d'une antenne directionnelle, on observe un gain de puissance par rapport à un émetteur isotrope. Ce gain est mesuré en décibels isotropes, notés dBi. Plus une antenne passive concentre le signal dans un faisceau étroit, plus le gain

de l'antenne est élevé. Il est important de retenir que le gain d'une antenne s'applique autant au signal émis qu'au signal reçu.

Prenons un exemple : si une antenne parvient à concentrer sans pertes l'ensemble de l'énergie de radiation dans un quart de sphère, alors la puissance perçue par un observateur situé dans le faisceau sera multipliée par quatre. Nous avons vu au chapitre 2 que multiplier la puissance par quatre équivaut à rajouter environ 6 décibels (c'est-à-dire $10 \times \log(4)$). Le gain d'une telle antenne serait alors de 6 dBi. Si vous trouvez une antenne dont le gain est de 20 dBi, vous pouvez faire le calcul inverse pour avoir une idée de la taille du faisceau obtenu : le faisceau sera concentré dans 1 % de la sphère.

> **Conclusion** : plus une antenne passive offre un gain important, plus le faisceau est étroit.

Théoriquement, les antennes parfaitement omnidirectionnelles n'offrent aucun gain, mais dans la pratique elles « aplatissent » le signal (elles rayonnent souvent peu vers le haut et vers le bas) : elles offrent donc également un gain. Cependant, le faisceau étant moins concentré, leur gain est en général plus faible que celui d'une antenne directionnelle.

Le PIRE

La puissance du signal perçu par un observateur est plus grande si ce signal est concentré en direction de l'observateur grâce à une antenne directionnelle et non diffusé de façon homogène dans l'espace. Si l'on remplace une antenne directionnelle par une antenne parfaitement omnidirectionnelle, il faut alors augmenter la puissance de l'émetteur pour que le récepteur perçoive la même puissance qu'auparavant. La puissance de cet émetteur omnidirectionnel équivalent est appelée la Puissance isotrope rayonnée équivalente (PIRE).

La loi française prend en compte le PIRE et non la puissance de l'émetteur. Par exemple, si l'on a un émetteur à 2,4 GHz d'une puissance de 30 mW (environ 15 dBm) relié à une antenne de 9 dBi, alors le PIRE est de 15 + 9 = 24 dBm, ce qui est supérieur à la limite de 20 dBm : on est dans l'illégalité et on risque une amende ! Ce calcul néglige toutefois la perte dans les connecteurs et le câble reliant l'émetteur à l'antenne. Si la perte est égale à 4 dB, alors le PIRE est égal à 20 dBm et tout va bien[1].

Diagramme de rayonnement

Dans la réalité, les antennes n'ont jamais un profil de rayonnement aussi simple qu'un faisceau homogène. Le cœur du faisceau est plus dense que la périphérie. La limite du faisceau n'est pas nette (fig. 4.19). Il y a souvent des lobes de rayonnement multiples. Ainsi, pour mieux connaître une antenne, on peut consulter son diagramme de rayonnement. Celui-ci montre avec précision une projection du rayonnement de l'antenne dans un plan (horizontal ou vertical). Le gain est parfois indiqué avec un

1. Voir le chapitre 11 pour plus de détails sur la réglementation.

dégradé de couleur, ou avec des courbes de niveau de gain, ou encore, le plus souvent, avec une seule courbe qui délimite la zone pour laquelle le gain est de 3 dBi inférieur au gain maximal (ou autres selon les diagrammes).

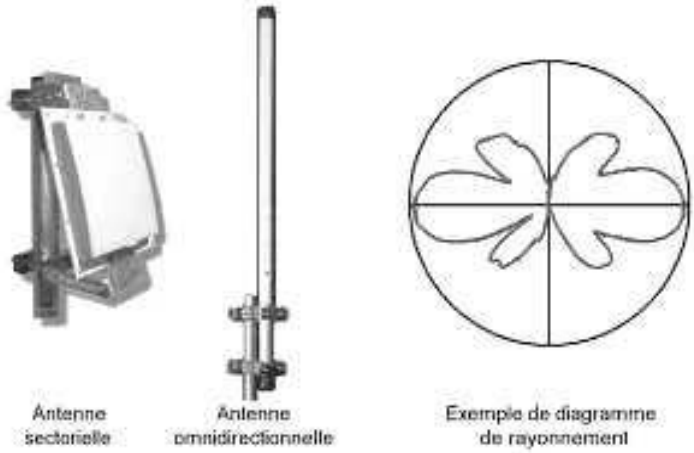


Figure 4.19 — Antennes et diagramme de rayonnement.

Lorsque ce diagramme n'est pas fourni, on peut obtenir une description simplifiée du faisceau :

- pour une antenne directionnelle, par l'angle horizontal et vertical du faisceau ;
- pour une antenne omnidirectionnelle, par l'angle vertical du rayonnement.

Ces angles ne donnent qu'une idée approximative du rayonnement réel. Le faisceau décrit par ces angles est en général délimité par la frontière de −3 dBi par rapport au gain maximal. Par exemple, si une antenne de 6 dBi a un faisceau de 60°, alors un observateur situé à 30° de l'axe de l'antenne n'aura un gain que de 3 dBi.

La bande passante

La dimension et la structure d'une antenne déterminent sa fréquence de résonance, c'est-à-dire la fréquence qu'elle émettra et qu'elle captera le mieux. Autour de cette fréquence de résonance, les fréquences voisines seront légèrement atténuées en émission comme en réception. La bande passante de l'antenne est la portion du spectre radio située autour de cette fréquence de résonance et pour laquelle l'atténuation est inférieure à une limite qu'on s'est fixée (en général 3 décibels).

Les antennes pour le WiFi sont donc en général spécialement conçues pour fonctionner soit à 2,4 GHz soit à 5 GHz, mais il existe quelques antennes bibandes.

La polarisation

Pour comprendre la polarisation en quelques mots, imaginez une corde tendue entre deux personnes : si l'une des personnes (l'émetteur) agite la corde de haut en bas, alors

une onde se forme et se propage le long de la corde. Le mouvement oscillatoire est vertical, donc on dit que la polarisation de l'onde est verticale. Si l'émetteur agite maintenant la corde de gauche à droite, la polarisation devient horizontale. Enfin, il peut appliquer en même temps un mouvement de haut en bas et de gauche à droite, pour créer une polarisation ellipsoïdale voire parfaitement circulaire. La polarisation circulaire peut être dans le sens des aiguilles d'une montre ou l'inverse : on parle de polarisation gauche ou droite.

Les ondes électromagnétiques peuvent elles aussi être polarisées horizontalement, verticalement, en diagonale ou bien selon un axe incliné quelconque. Elles peuvent également être polarisées de façon circulaire ou ellipsoïdale. Les formats d'antennes (voir paragraphes suivants) résultent en différentes polarisations du signal. Il va sans dire qu'une antenne à polarisation verticale aura une polarisation inclinée ou horizontale si on l'incline sur le côté !

On doit utiliser une antenne à polarisation verticale pour pouvoir correctement capter le signal émis par une autre antenne à polarisation verticale. De même pour la polarisation horizontale ou circulaire. Dans ce dernier cas, on doit avoir une antenne à polarisation circulaire gauche pour recevoir le signal d'une antenne à polarisation droite et *vice versa*.

4.4.2 Les formats d'antennes

Il existe une variété étourdissante d'antennes WiFi : antenne « fouet », antenne *patch*, parabole, parabole grillagée, antenne « yagi », antenne hélicoïdale, etc. Les passionnés de radio s'amusent en outre à fabriquer leurs propres antennes avec de simples boîtes de conserves et des trombones !

L'antenne fouet

L'antenne fouet est une simple tige métallique : c'est ce type d'antennes que l'on trouve sur les voitures. Sa longueur est un facteur simple de la longueur d'onde (par exemple le quart de la longueur d'onde). Elle est omnidirectionnelle, mais le signal est atténué verticalement. Elle peut ainsi aider à mieux couvrir un étage dans un bâtiment tout en limitant le débordement du signal aux étages voisins. On la place en général au centre d'une pièce, plutôt en hauteur (accrochée au plafond) pour éviter les obstacles.

La plupart des AP sont vendus avec une ou deux petites antennes de ce type, en général d'un gain de 2 à 3 dBi. Il existe également des antennes omnidirectionnelles en forme de longues barres de métal, utilisées à l'extérieur (pour couvrir un village par exemple), dont le gain peut aller jusqu'à 12 dBi ! D'une façon générale, quel que soit le type d'antenne, plus on souhaite un gain important, plus l'antenne doit être grande. La polarisation est celle de son axe : si elle est positionnée verticalement, la polarisation est verticale.

L'antenne patch

L'antenne patch est une plaque de métal carrée, en général de 10 à 20 cm de côté. Elle est sectorielle, avec un gain situé le plus souvent entre 6 et 15 dBi. Le produit le plus utilisé en entreprise est le patch de 6 dBi avec un faisceau de 60° horizontalement et 30° verticalement.

Le patch ne prend pas beaucoup de place et peut être fixé facilement sur un mur. Il peut également être intégré dans un faux plafond, ce qui limite l'impact visuel, diminue l'impact psychologique sur ceux qui craignent les méfaits pour la santé du WiFi et réduit le risque de vol. On la trouve souvent à l'extérieur, attachée en hauteur à un mât, pour couvrir un secteur important. Sa polarisation est également axiale.

Les paraboles

Les paraboles sont des antennes directionnelles ayant un gain compris le plus souvent entre 13 et 24 dBi. Ce sont les mêmes types d'antennes utilisées pour la télévision par satellite par exemple. Il existe des variantes grillagées, moins coûteuses, offrant moins de prise au vent. Elles ont souvent entre 30 cm et 1 m de diamètre, ce qui les rend difficiles à installer et à régler. Elles servent donc essentiellement à établir des liaisons de point à point entre des bâtiments distants. Leur polarisation est à nouveau axiale.

Les antennes Yagi

Les antennes Yagi sont des antennes directionnelles en forme de « râteau » : elles sont constituées d'une tige à laquelle sont accrochées perpendiculairement plusieurs tiges métalliques de longueur variable. La bande passante et le diagramme de rayonnement sont déterminés par la longueur de ces tiges et leur espacement. Elles sont peu coûteuses et offrent un gain assez important. Ce type d'antennes est souvent utilisé pour capter la télévision hertzienne, par exemple. Leur polarisation est encore une fois axiale.

Les antennes hélicoïdales

Les antennes hélicoïdales sont directionnelles, elles aussi, mais leur forme en tire-bouchon leur confère une propriété bien utile : le signal émis a une polarité circulaire. Elles permettent de réduire les problèmes de réception liés aux réflexions, pour du point à point en milieu urbain en particulier. Nous approfondirons ceci au chapitre 5.

Les antennes « intelligentes »

Il existe une foule d'autres types d'antennes qu'il serait inutile de décrire ici. Mentionnons toutefois les antennes « intelligentes » qui émettent les paquets de données dans la direction du récepteur. Cela donne un gain important à l'antenne, tout en offrant une capacité équivalente à plusieurs AP simultanés. Cela rend ce type d'antennes intéressantes pour couvrir des villages avec une seule antenne, par exemple. Malheureusement, ces antennes sont en général assez chères et ont un gain trop important pour la législation française.

4.4.3 Les câbles et les connecteurs d'antennes

Pour relier une antenne à un adaptateur WiFi ou à un AP, on utilise en général des câbles coaxiaux (du fait de leur faible impédance). L'atténuation du signal dépend du produit choisi et se situe en général entre 0,2 dB par mètre de câble et 1 dB/m. Il est recommandé de limiter autant que possible la distance entre l'émetteur et l'antenne, afin d'éviter de perdre une trop grande partie du signal dans le câble, mais aussi car plus le câble est long, plus il est sensible au bruit électromagnétique ambiant. C'est pourquoi les câbles d'antennes se vendent parfois sous la forme de petits câbles d'une vingtaine de centimètres de long seulement : on les appelle les *pigtails*, c'est-à-dire les « queues de cochons » (fig. 4.20).

Figure 4.20 — Exemples de connecteurs d'antennes.

Il existe plusieurs types de connecteurs d'antennes, dont certains sont limités à un seul constructeur. En achetant une antenne et un câble pour un AP ou un adaptateur WiFi, assurez-vous que leurs connecteurs soient compatibles. Les plus répandus en France sont les suivants (chacun ayant sa version mâle et femelle) :

- SMA et SMA inversé (*Reverse SMA* ou R-SMA) ;
- N ;
- M ;
- MMCX ;
- TNC et TNC inversé (RP-TNC) ;
- MC-Card pour se connecter aux cartes Orinoco/Avaya/Lucent.

4.5 LE MATÉRIEL POUR LE DÉPLOIEMENT

4.5.1 Le PoE

Principe du PoE

Lors d'un déploiement WiFi d'envergure, s'il faut installer une vingtaine d'AP, le plus coûteux sera souvent l'installation du câblage électrique et Ethernet (pour relier les AP au réseau filaire). Une façon de réduire ce coût est d'apporter l'alimentation électrique des AP au travers des câbles Ethernet ! Cette technologie s'appelle le *Power over Ethernet* (PoE) et elle a été standardisée par l'IEEE sous le nom 802.3af. Son essor actuel s'explique sans doute en partie par son utilité dans les déploiements WiFi !

Le principe du PoE est le suivant : un équipement appelé l'« injecteur » est alimenté électriquement et reçoit en entrée un câble Ethernet classique. Sur un

deuxième câble Ethernet tout à fait classique, il émet les données reçues (courant faible) ainsi que le courant électrique (courant fort). À l'arrivée, un « séparateur » effectue l'opération inverse : il reçoit en entrée le câble Ethernet venant de l'injecteur et il sépare l'électricité (vers une prise électrique) et les données (vers un câble Ethernet).

Il existe également des injecteurs à ports multiples : ce sont des commutateurs classiques mais leurs ports sont compatibles 802.3af. Cela permet d'alimenter avec un seul injecteur plusieurs équipements. Un autre avantage est de pouvoir gérer de façon centralisée l'alimentation électrique d'équipements distribués dans tout un bâtiment. Ceci permet, entre autres, de n'avoir qu'un seul onduleur[1] pour tous les équipements reliés à l'injecteur multiple.

Figure 4.21 — Exemples de produits *Power over Ethernet* (PoE).

Certains équipements, dont des AP, des téléphones sur IP ou encore des caméras de surveillance, intègrent un séparateur 802.3af, ce qui permet de les brancher directement au câble Ethernet sortant de l'injecteur, sans passer par un séparateur externe.

Malheureusement, l'intensité du courant est limitée à 350 milliampères (mA) par le 802.3af et la puissance continue maximale que l'on peut apporter à un équipement au travers d'un câble Ethernet, compte tenu des pertes dans le câble Ethernet, est de 12,95 W. Or, un point d'accès consomme en général environ 10 W, ce qui signifie qu'un port d'injecteur ne peut alimenter qu'un seul AP : on ne peut en principe pas chaîner deux AP à partir d'un même port de l'injecteur.

Fonctionnement du PoE

Le 802.3af définit deux façons de faire passer le courant fort sur un câble Ethernet :

- la première consiste à simplement utiliser l'une des paires torsadées libres du câble Ethernet : en effet, sur les quatre paires de cuivres, seules deux sont utilisées par le standard Ethernet ;

1. Un onduleur est un équipement qui fournit une alimentation électrique de secours pendant quelques minutes (ou quelques heures selon les produits) pendant une coupure de courant et protège contre les surtensions (orages...).

- la seconde utilise les mêmes paires pour transporter le courant fort et le courant faible, en les superposant. Cette deuxième méthode semble avoir la préférence de l'industrie, sans doute parce qu'elle économise les paires de cuivre libres, qui peuvent ainsi être employées à d'autres fins.

Le standard 802.3af définit un mécanisme de détection automatique de la méthode de transmission du courant utilisée. En outre, avant d'envoyer du courant fort sur un câble Ethernet, un injecteur 802.3af vérifie toujours si l'équipement branché à l'autre extrémité du câble en question est bien compatible avec le 802.3af (grâce à l'échange d'une « signature » 802.3af) : ceci permet d'éviter d'endommager des équipements branchés à l'injecteur et incompatibles avec le PoE.

Attention : tous les produits PoE ne respectent pas la norme 802.3af. Certains injecteurs et séparateurs sont mis en œuvre par les constructeurs d'AP et ne sont utilisables qu'avec ces AP.

Ces produits « propriétaires » peuvent avoir quelques atouts, comme la possibilité de transporter davantage de puissance électrique pour pouvoir chaîner deux voire trois AP avec un seul câble Ethernet, mais il faut faire attention à ne rien brancher d'autre que les équipements prévus à cet effet.

4.5.2 Le CPL

Le Courant porteur en ligne (CPL) est une technologie symétrique au PoE : elle permet de transporter des données sur l'installation électrique d'un bâtiment.

Selon la configuration du site que l'on doit couvrir en WiFi, il peut arriver que le CPL permette d'économiser un câblage Ethernet coûteux pour relier plusieurs AP entre eux. Le débit maximal offert par le CPL est toutefois limité à 14 Mb/s ce qui est assez faible dans un contexte d'entreprise. En outre, comme nous l'avons vu, le CPL n'est pas toujours possible, selon l'installation électrique du bâtiment et un test s'impose avant d'opter pour cette solution technique. Le CPL reste une solution simple d'interconnexion entre les AP pour un contexte familial ou un petit bâtiment.

4.5.3 Les filtres passe-bande et les atténuateurs

Pour clore ce chapitre dédié au matériel WiFi, mentionnons deux outils parfois utiles pour les déploiements radio : les filtres passe-bande et les atténuateurs.

Les filtres passe-bande se branchent à une antenne WiFi et permettent de filtrer physiquement les interférences provenant des ondes situées hors de la bande de fréquence utilisée. Les adaptateurs WiFi intègrent souvent un filtre, mais leur qualité n'est pas toujours optimale : ce filtre s'applique en général à l'ensemble du spectre et non au canal utilisé. Installer un filtre peut permettre d'améliorer le Rapport signal/bruit (RSB) à la réception dans un environnement bruyant ;

Les atténuateurs permettent de simuler une longueur plus ou moins importante de câble d'antenne en atténuant le signal. C'est un outil utile pendant un audit de site

pour savoir où il sera le plus judicieux de placer une antenne : proche de l'émetteur mais loin de la zone à couvrir, ou *vice versa*.

Résumé

Dans ce chapitre, nous avons présenté cinq catégories principales de matériel WiFi : les adaptateurs, les points d'accès, les périphériques, les antennes et le matériel pour le déploiement WiFi.

Les adaptateurs mettent en œuvre le 802.11 pour permettre à un équipement de communiquer en WiFi. Ils se présentent sous diverses formes : cartes PCMCIA, PCI ou encore Compact Flash, bundles ou sticks USB, petits boîtiers à connecter au port Ethernet, etc. Nous avons parlé des *firmwares*, des pilotes et de l'importance de l'interface de l'utilisateur.

Les points d'accès sont de plusieurs types :

– **AP pont vers un réseau filaire** – Un pont est en général assez malin pour ne relayer vers le réseau filaire que le trafic qui doit l'être et *vice versa*.

– **AP répétiteur** – Il peut être relié sans fil à un ou plusieurs autres AP et étendre ainsi la couverture d'un réseau sans fil sans avoir à être relié directement au réseau filaire.

– **AP routeur** – Il s'agit d'un produit deux en un : un AP et un routeur IP classique, permettant de connecter le réseau sans fil à Internet ou bien à un autre réseau IP. Il possède les fonctions habituelles d'un routeur, telles qu'un serveur DHCP, un pare-feu ou encore le NAT.

– **Hotspot-in-a-box** – C'est un AP routeur intégrant un contrôleur d'accès pour *hotspot*. Il peut mettre en œuvre des fonctions avancées telles que l'authentification des clients par portail captif en HTTPS (éventuellement en interrogeant un serveur RADIUS ou LDAP), la transparence SMTP ou proxy, etc.

Nous avons également abordé certaines fonctions avancées des AP, telles que la gestion du protocole STP, la possibilité de mettre en œuvre plusieurs SSID, chacun ayant son propre modèle de sécurité (ouvert, WEP, WPA...), son propre VLAN associé, ses propres règles de QoS, etc.

Les périphériques WiFi que nous avons présentés sont nombreux : les ordinateurs, Tablet PC, PDA et smartphones, les imprimantes, les vidéoprojecteurs, les caméras, le matériel multimédia comme les chaînes Hi-Fi WiFi, les analyseurs complets et les simples détecteurs de réseaux sans fil, les lecteurs sans fil, les outils de localisation et enfin les téléphones sur WiFi. Le WiFi permet à tout et n'importe quoi de se connecter sans fil.

Les antennes WiFi peuvent être actives ou passives, mais on n'installe que des antennes passives pour le WiFi, étant donnée la législation assez restrictive en termes de puissance d'émission. Une antenne doit être choisie en fonction de sa bande passante (2,4 GHz, 5 GHz ou compatible avec les deux), sa directivité, son gain, son diagramme de rayonnement ou sa polarisation. Les formats d'antennes sont nombreux mais le plus utilisé en entreprise reste le patch, qui s'intègre facilement

dans un faux plafond. Une fois l'antenne sélectionnée, il faut encore choisir le bon connecteur d'antenne, adapté d'un côté à l'AP ou à l'adaptateur WiFi et de l'autre à l'antenne.

Pour finir, nous avons présenté quelques produits utiles pour le déploiement WiFi : les injecteurs et séparateurs PoE, qui permettent de faire passer du courant électrique sur des câbles Ethernet ; les adaptateurs CPL, pour utiliser l'installation électrique d'un bâtiment comme un réseau local ; les filtres passe-bande, pour améliorer la qualité du signal dans un environnement électromagnétique bruyant ; les atténuateurs, qui peuvent simuler l'effet de l'installation d'un long câble d'antenne.

5

La couverture radio

Objectif

Comment réussir une liaison de point à point à haut débit sur une grande distance ? Quelles antennes choisir ? Comment respecter la limite de puissance légale tout en optimisant la portée ? Comment limiter le nombre de points d'accès à installer tout en ayant une bonne couverture radio ? Comment obtenir une grande capacité et gérer de nombreux utilisateurs ? Pour répondre à toutes ces questions et bien d'autres encore, nous commencerons par étudier la propagation des ondes radio et passerons ensuite au déploiement en entreprise. Pour aborder les ondes radio, nous partirons du cas le plus simple à modéliser : la liaison de point à point, avec un seul point d'accès (AP) et un seul utilisateur. Nous étudierons tous les facteurs qui jouent sur une liaison radio : la puissance des émetteurs, le gain des antennes, la sensibilité des récepteurs, mais aussi l'absorption, la réflexion, la diffraction et la polarisation. Le but est de vous donner une bonne compréhension des ondes radio pour vous permettre de faire les bons choix lors de votre déploiement. Par la suite, nous aborderons le cas qui vous concerne sans doute plus directement que le point à point : le déploiement de multiples AP en entreprise, pour réaliser un réseau performant et stable.

5.1 LE BILAN RADIO

5.1.1 Un schéma général

Le chemin du signal

Une émission radio d'un point X à un point Y peut être modélisée de la façon suivante :

- **L'émetteur** produit le signal sous la forme d'un courant électrique d'une puissance P_X donnée (qui est indiquée sur la documentation du produit, par exemple 15 dBm).
- **Le câble d'antenne** relaie ce signal électrique jusqu'à l'antenne d'émission, avec une certaine perte de puissance C_X, proportionnelle à la longueur du câble. On perd en général environ 0,2 à 1 dB de puissance par mètre de câble, selon sa qualité.
- **L' antenne d'émission** rayonne le signal dans l'espace sous la forme d'ondes électromagnétiques, en les concentrant plus ou moins dans la direction du récepteur, d'où un gain de puissance apparent pour le récepteur G_X (voire une perte, s'il n'est pas dans l'axe de l'antenne d'émission). Le gain de l'antenne (par exemple 6 dBi) et parfois également son diagramme de rayonnement sont fournis par le vendeur.
- **La puissance du signal** s'atténue de façon proportionnelle au carré de la distance parcourue, ce qu'on appelle « l'affaiblissement en espace libre ».
- **L'antenne de réception** capte les ondes électromagnétiques et les transforme en courant électrique, en offrant encore éventuellement un gain de puissance G_Y (ou une perte si l'antenne est mal orientée).
- **Le signal électrique** est véhiculé par un câble d'antenne vers le récepteur, à nouveau avec une perte de puissance C_Y.
- Enfin, **le récepteur**, selon sa sensibilité S_Y (par exemple −90 dBm), parvient ou non à capter le signal électrique qu'il reçoit.

Pour que Y puisse recevoir le signal émis par X, il faut que la formule suivante soit vérifiée (tout étant exprimé en décibels) :

$$P_X + C_X + G_X + A + G_Y + C_Y > S_Y$$

On peut également calculer la marge M_{XY}, qui doit donc être positive :

$$M_{XY} = P_X + C_X + G_X + A + G_Y + C_Y - S_Y > 0$$

Attention : les paramètres C_X, A, C_Y et S_Y ont chacun une valeur négative.

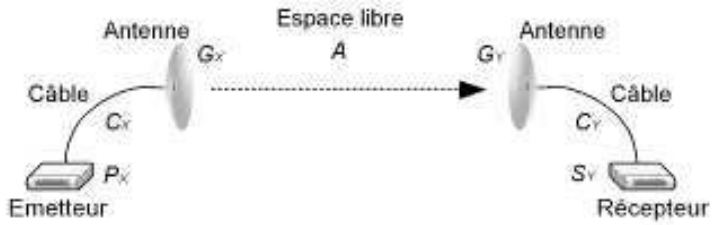


Figure 5.1 — Le bilan radio.

L'affaiblissement en espace libre

Pour évaluer l'affaiblissement en espace libre, on utilise la formule suivante, déduite de la formule de Friis, qui est plus générale :

$$A = 20 \times \log\left(\frac{4\pi}{\lambda}\right) + 20 \times \log(d)$$

d est la distance entre l'émetteur et le récepteur, en mètres ;
λ est la longueur d'onde du signal, en mètres.

On obtient donc les formules suivantes, selon la fréquence :

- Fréquence de 2,4 GHz : $A = 40{,}0 + 20 \times \log(d)$
- Fréquence de 5 GHz : $A = 46{,}4 + 20 \times \log(d)$

Par exemple, en utilisant le 802.11b, c'est-à-dire à 2,4 GHz, on perd environ 100 dB si la distance entre l'émetteur et le récepteur est de 1 000 mètres. *Attention*, il ne faut pas en déduire que l'on perd 200 dB sur 2 000 mètres ! En effet, en doublant la distance, on perd seulement $20 \times \log(2) = 6$ dB de plus. Si la distance est de 2 000 mètres, on perd donc 106 dB, si elle est de 4 000 mètres, on perd 112 dB, etc.

Notez que l'affaiblissement en espace libre est nettement plus important à 5 GHz qu'à 2,4 GHz : 6,4 dB de plus !

> La portée d'un signal à 5 GHz est inférieure à la moitié de la portée d'un signal à 2,4 GHz, toutes choses égales par ailleurs.

Communication bilatérale

Grâce à ce modèle et à ces formules, on peut faire ce qu'on appelle le « bilan radio » : il s'agit de chiffrer chacune des étapes et d'en déduire si la communication pourra avoir lieu ou non.

Dans le cas de la télévision hertzienne, la communication est à sens unique : il suffit que le récepteur puisse « entendre » l'émetteur pour que le système fonctionne. En revanche, le WiFi suppose des échanges bilatéraux : lors d'une communication entre deux stations, il est donc nécessaire que chaque station soit en mesure de capter le signal de l'autre[1]. Pour déterminer si la communication est envisageable, il faut faire le bilan radio dans chacun des deux sens.

> Pour qu'une communication WiFi puisse avoir lieu, il faut que le bilan radio soit satisfaisant dans les deux sens.

1. À part bien sûr dans le cas où le récepteur ne fait qu'écouter (sniffer) le réseau à des fins d'analyse.

5.1.2 Un exemple de point à point

Le village WiFi

Pour bien comprendre le bilan radio, nous allons prendre un exemple concret. Imaginons qu'un AP (station X) soit relié à Internet et placé au centre d'un village. Cet AP utilise le 802.11b et a une puissance d'émission P_X = +15 dBm (environ 30 mW) et une sensibilité S_X = −90 dBm (pour un débit de 1 Mb/s, le minimum possible). Il est relié à une antenne sectorielle (de type patch) offrant un gain G_X = +6 dBi. Celle-ci est installée sur un mât en hauteur afin d'éviter tout obstacle et elle est pointée parfaitement vers les habitations. Le câble d'antenne atténue la puissance du signal de C_X = −2 dB.

David habite en périphérie de ce village et souhaite bénéficier de la connexion à Internet *via* le WiFi. Son domicile se trouve à d = 2 000 mètres de l'AP, d'où une atténuation en espace libre de A = −106 dB. Par chance, il est parfaitement dans l'axe de l'antenne du point d'accès.

Il achète donc un adaptateur WiFi USB et le connecte à son ordinateur (station Y). Ce petit boîtier a une puissance d'émission P_Y = +20 dBm (100 mW) et une sensibilité pour 1 Mb/s de S_Y = −92 dBm. Il installe une antenne directionnelle de type Yagi (voir le chapitre 4), d'un gain G_Y = +8 dBi, sur son toit, en la pointant vers l'antenne de l'AP. Malheureusement, l'ordinateur de David se trouve au rez-de-chaussée et le câble USB de l'adaptateur WiFi n'est pas assez long. Du coup, il achète un câble d'antenne d'une longueur de 10 mètres et relie son adaptateur à l'antenne sur le toit. Ce câble est de qualité médiocre, entraînant une perte de 1 dB par mètre, c'est-à-dire au total une perte de C_Y = −10 dB dans le câble d'antenne.

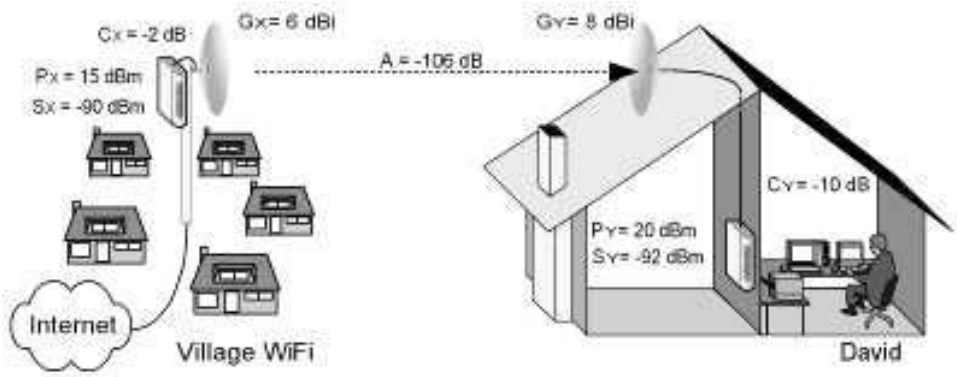


Figure 5.2 — Exemple de déploiement WiFi dans un village.

Calcul du bilan radio

Avec tous ces éléments nous pouvons faire le bilan radio de l'AP vers David, puis de David vers l'AP : les deux doivent être satisfaisants pour que la communication soit possible.

1. De l'AP vers David, c'est-à-dire de la station X à la station Y, on peut estimer la marge dont on dispose :

$$\begin{aligned} M_{XY} &= P_X + C_X + G_X + A + G_Y + C_Y - S_Y \\ &= +15 - 2 + 6 - 106 + 8 - 10 + 92 \\ &= +3\ dBm \end{aligned}$$

   La communication devrait être possible dans ce sens à 1 Mb/s, car la marge est positive.

2. Dans l'autre sens, c'est-à-dire de la station Y vers la station X, on peut également estimer la marge disponible :

$$\begin{aligned} M_{XY} &= P_Y + C_Y + G_Y + A + G_X + C_X - S_X \\ &= +20 - 10 + 8 - 106 + 6 - 2 + 90 \\ &= +6\ dBm \end{aligned}$$

   Même logique : puisque la marge est positive, la communication devrait être possible de Y vers X.

Qu'est-ce qu'une bonne marge ?

David fait ces calculs et croit que la communication sera bonne car il y a de la marge dans les deux sens. Malheureusement, ce sont des approximations basées sur un modèle théorique : dans la pratique, les interférences, les obstacles, l'orientation des antennes (si le récepteur n'est pas parfaitement dans l'axe), une légère inclinaison des antennes (si l'antenne de réception n'est pas dans l'axe de polarisation du signal radio émis), l'humidité de l'air et toutes sortes d'autres facteurs peuvent amener à revoir à la baisse ces estimations.

Du coup, il vaut mieux avoir une marge plus importante pour s'assurer que la pratique rejoindra la théorie : une marge de 6 dBm est souvent considérée comme un minimum. Avec une marge plus faible, la communication sera parfois impossible, ou très instable... mais seule l'expérience pourra confirmer cette affirmation !

> Une marge de 6 dBm est en général considérée comme le minimum pour garantir une connexion stable.

5.1.3 Comment améliorer le bilan radio ?

Les axes d'amélioration

Dans notre exemple précédent, il est donc peu probable que la communication soit satisfaisante, car la marge est trop faible de X vers Y (de l'AP vers David). Comment David peut-il résoudre ce problème ? Il a heureusement de nombreuses options, toutes complémentaires :

- il peut acheter une antenne plus puissante pour améliorer à la fois l'émission et la réception ;
- il peut acheter du câble d'antenne de meilleure qualité pour qu'il y ait moins de pertes entre son antenne et son récepteur ;
- il peut essayer de raccourcir autant que possible le câble d'antenne en rapprochant l'adaptateur de l'antenne. Il peut par exemple déplacer son ordinateur et son adaptateur au dernier étage plutôt qu'au rez-de-chaussée, ou bien installer uniquement l'adaptateur au dernier étage et le relier à l'ordinateur au rez-de-chaussée avec une rallonge USB. Une autre solution consiste donc à acheter un adaptateur Ethernet (voir le chapitre 4), à l'installer au dernier étage et à le relier à l'ordinateur au rez-de-chaussée avec un long câble Ethernet ;
- il peut acheter un adaptateur WiFi ayant une meilleure sensibilité et pourquoi pas une plus grande puissance (bien que le problème soit plutôt à la réception dans notre exemple).

Attention au PIRE

En installant une antenne et un émetteur plus puissants, ou encore en diminuant la perte dans le câble d'antenne, on change naturellement la Puissance isotrope rayonnée équivalente (*PIRE*) du système (voir le chapitre 4). Le PIRE d'une station se calcule grâce à la formule suivante :

$$PIRE = P + C + G$$

Dans notre exemple, le PIRE des stations X et Y se calcule donc ainsi :

$$PIRE_X = P_X + C_X + G_X = +15 - 2 + 6 = +19\ dBm$$
$$PIRE_Y = P_Y + C_Y + G_Y = +20 - 10 + 8 = +18\ dBm$$

La limite légale pour le 2,4 GHz étant en France de 20 dBm[1], on est dans la légalité des deux côtés. Mais si David remplace son antenne par une antenne à 15 dBi, par exemple, il réglera certes ses problèmes de réception, mais il dépassera largement le PIRE maximal autorisé à l'émission !

Améliorer la transmission dans la légalité

La question est donc la suivante : comment David peut-il obtenir la meilleure transmission possible (en réception et en émission) tout en restant dans la légalité ?

Si l'on suppose qu'il ne peut rien faire au niveau de la station X (qui est gérée par la mairie, par exemple), le problème revient à optimiser les paramètres de la station Y : la sensibilité du récepteur (S_Y), la puissance de l'émetteur (P_Y), la perte dans le câble d'antenne (C_Y) et le gain de l'antenne (G_Y). Pour atteindre la limite légale sans la dépasser, il faut que le PIRE de David soit égal à 20 dBm, c'est-à-dire simplement :

$$PIRE_Y = P_Y + C_Y + G_Y = 20\ dBm$$

1. Pour les canaux 1 à 7, voir les tableaux synthétiques concernant la législation au chapitre 11.

Si la puissance de l'émetteur augmente, il faut donc le compenser par davantage de pertes dans le câble ou bien une antenne à plus faible gain. De même, si le gain de l'antenne augmente, il faut diminuer la puissance de l'émetteur ou augmenter la perte dans le câble. Alors que choisir ? Un émetteur puissant ? Une antenne à haut gain ? Un câble à faible perte ? La réponse peut être déduite des formules du bilan radio.

Commençons par la transmission de Y vers X. Le bilan radio dans ce sens s'exprime par la formule suivante, si l'on admet que le $PIRE_Y$ (du système de David) est égal à 20 dBm :

$$\begin{aligned} M_{YX} &= P_Y + C_Y + G_Y + A + G_X + C_X - S_X \\ &= PIRE_Y \qquad + [\textit{paramètres non modifiables par David}] \end{aligned}$$

On voit que la puissance reçue par l'AP ne dépend que du PIRE du système de David. Donc, pour la transmission vers l'AP, peu importe que David ait une antenne à haut gain ou un émetteur puissant ou encore un câble à faibles pertes pourvu que son $PIRE_Y$ soit maximal, c'est-à-dire égal à 20 dBm (pour le 2,4 GHz).

Maintenant dans l'autre sens, de X vers Y, la marge s'exprime par la formule :

$$\begin{aligned} M_{XY} &= P_X + C_X + G_X + A + G_Y + C_Y - S_Y \\ &= PIRE_X \qquad + A + G_Y + C_Y - S_Y \\ &= [\textit{non modifiable}] \; + G_Y + C_Y - S_Y \end{aligned}$$

On voit que pour améliorer la transmission de X vers Y, il faut que l'antenne de David ait un gain aussi élevé que possible (G_Y maximal), qu'il y ait peu de pertes dans le câble d'antenne (C_Y proche de 0 dB) et que la sensibilité du récepteur soit excellente (S_Y très bas).

Pour avoir la meilleure communication possible, dans les deux sens, David doit configurer son installation de telle sorte que :

- S_Y soit bas, pour une meilleure sensibilité de réception : par exemple −94 dBm ;
- C_Y soit très proche de 0 dB : dans la pratique, on a rarement moins de 2 dB ;
- G_Y soit aussi grand que possible : par exemple, 22 dBm ;
- $PIRE_Y$ soit égal à la limite légale donc $P_Y = PIRE_{max} - C_Y - G_Y$.

Pour une connexion de point à point, il vaut mieux utiliser des antennes à haut gain, des câbles courts et à faible perte, des récepteurs très sensibles, et enfin, pour ne pas dépasser le PIRE légal, des émetteurs peu puissants.

Détaillons ce dernier point : la puissance de l'émetteur (P_Y) doit être assez faible pour éviter de dépasser le PIRE maximal autorisé. Par exemple, avec C_Y = 2 dB et G_Y = 20 dBm, on doit avoir P_Y = 0 dBm, c'est-à-dire 1 mW. Notez que 0 dBm ne correspond pas à 0 mW, mais bien à 1 mW ! On peut même théoriquement avoir des émetteurs d'une puissance inférieure à 0 dBm, par exemple −10 dBm, soit 0,1 mW.

Dans la pratique, les émetteurs WiFi ont en général une puissance comprise entre 15 dBm ou 20 dBm et certains peuvent être réglés pour se limiter à 10, 5, 1, voire 0 dBm. Ces derniers sont en général assez chers, donc on peut être tenté d'acheter un AP à 15 dBm et d'installer un câble d'antenne à perte importante ou une antenne moins puissante pour ne pas dépasser le PIRE légal. Malheureusement, cela diminuera d'autant l'émission et la réception !

Angle ouvert ou fermé

Pour obtenir la meilleure communication possible entre deux points, on a vu qu'il fallait que les câbles d'antennes soient aussi courts que possible et la sensibilité des récepteurs aussi bonne que possible. En outre, puisqu'on est limité par un PIRE maximal, il vaut mieux avoir une antenne à haut gain (qui agit à la fois à la réception et à l'émission) plutôt qu'un émetteur puissant (qui ne joue qu'à l'émission).

Mais il y a une limite à ce dernier point : si le signal produit par l'émetteur est très faible, alors l'antenne amplifiera bien ce signal mais elle amplifiera avec lui le bruit présent dans le câble, ce qui augmente le rapport signal/bruit. Il faut donc trouver un bon équilibre entre puissance de l'émetteur et gain de l'antenne en fonction du RSB mesuré.

En outre, plus l'antenne a un gain important, plus son faisceau de rayonnement est étroit. Ceci n'est pas gênant voire même souhaitable dans une connexion fixe de point à point, mais ce n'est pas toujours idéal, en particulier si les utilisateurs sont mobiles, ou bien s'ils peuvent se situer tout autour de l'AP. Pour un angle très ouvert, on choisira donc une antenne omnidirectionnelle à gain moyen (2 à 5 dBi) et pour compenser, un émetteur relativement puissant (15 à 20 dBm). Inversement, pour un angle fermé (point à point), on choisira une antenne directionnelle à haut gain (9 à 20 dBi) et du coup un émetteur faible (0 à 8 dBm). Dans notre exemple, l'AP est dans le premier cas (elle doit rayonner sur l'ensemble du village) alors que le système de David est manifestement dans le second cas (il est fixe et toujours pointé vers l'AP).

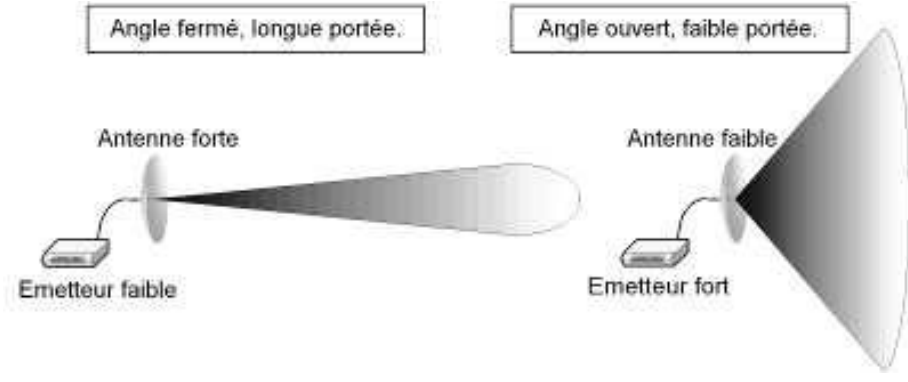


Figure 5.3 — Les antennes et l'angle de rayonnement.

5.2 LES PERTURBATIONS RADIO

Malgré un bilan radio satisfaisant, un certain nombre de perturbations peuvent venir altérer les prédictions : le bruit, les obstacles, les réflexions, la polarisation et la diffraction. Comment optimiser une connexion en tenant compte de ces nouveaux paramètres ?

5.2.1 Le bruit et les interférences

Le bruit peut perturber énormément les communications en provoquant une perte importante de paquets. Si le RSB n'est pas suffisamment élevé, la communication ne sera tout simplement pas possible, même si le signal reçu a une puissance importante.

Les réseaux voisins

La première source de bruit pour le WiFi est... le WiFi ! Si un voisin a déployé un réseau WiFi et que certains de ses AP utilisent des canaux proches ou identiques à ceux de vos AP, alors vous subirez des pertes importantes de débit (et lui aussi).

La première chose à faire avant un déploiement est de faire un « audit de site », c'est-à-dire une cartographie radio du site à déployer. Entre autres, cet audit de site permettra de vérifier s'il existe des réseaux voisins, sur quels canaux, à quelle puissance, etc. Pour cela, on peut utiliser un analyseur du type NetStumbler ou AirMagnet pour ne citer qu'eux. Ils permettent de savoir si un AP est déployé à proximité, quel canal il utilise et plus généralement quel est le RSB sur un canal donné. Certains outils permettent même de mesurer précisément quelle est la perte réelle de trames ou *Frame Error Rate* (FER), sur un canal donné, ou encore la perte de bits d'information ou *Bit Error Rate* (BER). Nous reparlerons de ces outils et de l'audit de site au § 5.3.4.

Si le propriétaire du réseau voisin peut être identifié, n'hésitez pas à le contacter et à vous arranger à l'amiable avec lui pour vous répartir les canaux disponibles. Si le PIRE de son système dépasse la limite autorisée, la loi est bien sûr de votre côté, mais une simple discussion suffit en général à résoudre le problème sans avoir à faire appel à la police ! Bref, il s'agit d'une relation de voisinage tout à fait classique.

Ensuite, il faut configurer chaque AP sur un canal libre et peu bruyant. Si vous utilisez le 802.11b ou le 802.11g, il faut choisir des canaux assez éloignés de ceux qui sont déjà occupés, car les canaux voisins se superposent : idéalement, il faut au moins cinq canaux d'écart avec un canal occupé. Le problème ne se pose pas avec le 802.11a car tous les canaux sont indépendants : il suffit donc de choisir un canal inoccupé.

Le Bluetooth

Claviers, souris, imprimantes, PDA, ordinateurs et autres matériels utilisant la technologie Bluetooth peuvent perturber le 802.11b et le 802.11g car ils emploient la même bande de fréquences à 2,4 GHz. Puisque cette technologie repose sur la modulation FHSS (voir le chapitre 2, § 2.3.3), l'ensemble des canaux WiFi est touché.

Heureusement, la puissance des équipements Bluetooth est en général assez faible, donc le problème ne se pose que si l'on est à proximité (moins d'une dizaine de mètres) d'un équipement Bluetooth. Par ailleurs, l'utilisation de ces équipements est en général ponctuelle : synchronisation d'un PDA avec un ordinateur, échange de cartes de visites électroniques entre ordinateurs et ainsi de suite, donc le problème est souvent si limité dans le temps qu'on ne le remarque pas.

Toutefois, si votre société a déployé un réel réseau d'antennes Bluetooth, par exemple pour permettre à tous les employés de synchroniser leurs PDA à tout moment, alors le risque d'interférences est énorme : c'est le cas par exemple dans certains hôpitaux américains dans lesquels les docteurs peuvent mettre à jour leurs rendez-vous sur leurs PDA, où qu'ils se trouvent. Par ailleurs, si un équipement Bluetooth est fréquemment utilisé par vos employés et pendant des durées importantes, comme des oreillettes sans fil permettant de téléphoner sur IP, par exemple, alors les risques d'interférences sont importants.

Une solution consiste à définir des règles d'usage des ondes radio au sein de votre entreprise, par exemple en n'autorisant l'utilisation du Bluetooth que pour synchroniser des PDA. Par ailleurs, certains produits Bluetooth savent détecter et éviter les canaux occupés par le WiFi.

Une autre alternative est d'utiliser le 802.11a ou le 802.11n à 5 GHz, car à ces fréquences on n'est pas du tout gêné par le Bluetooth. Rappelons toutefois que le 802.11a est très peu répandu actuellement en France car il est incompatible avec le 802.11b et le 802.11g et était interdit à l'extérieur jusqu'en janvier 2006. Les équipements 802.11n à 5 GHz sont également assez rares pour l'instant.

> Le Bluetooth peut considérablement nuire au débit de votre réseau WiFi, s'il est utilisé intensivement. Il touche tous les canaux à 2,4 GHz.

Les fours à micro-ondes

Ne souriez pas, une autre source de bruit très sérieuse est le four à micro-ondes. En effet, ces fours sont présents chez beaucoup de particuliers et dans de nombreuses cafétérias d'entreprises. Ils provoquent fréquemment des problèmes importants d'interférences avec le WiFi car ils sont extrêmement bruyants sur les fréquences de 2,4 GHz. En outre, on ne les remarque pas toujours pendant l'audit de site, car ils ne sont pas utilisés en permanence. Une fois déployé, le réseau sans fil fonctionne correctement la plupart du temps, mais aux alentours de midi, tous les jours, à plusieurs reprises et sans raison apparente, le réseau sans fil devient extrêmement lent voire indisponible pendant quelques minutes : à cette heure-ci, les employés font chauffer leur repas !

Heureusement, la fréquence radio exacte utilisée par un four est en général indiquée à l'arrière du four ou dans sa documentation : on doit essayer d'utiliser les canaux les plus éloignés possible de cette fréquence. Le plus sûr est de le mettre en marche pendant les tests préalables au déploiement (ne le faites pas tourner à vide, cela pourrait l'endommager). Encore une fois, le 802.11a n'est pas touché, de même que le 802.11n à 5 GHz.

Attention : la plupart des outils d'audit de sites n'analysent que l'environnement WiFi, et sont incapables de détecter le Bluetooth, les micro-ondes et les autres sources d'interférences telles que les équipements de vidéosurveillance sans fil ou certains équipements de détection d'intrusions. De même, certains AP ont une option de sélection automatique du canal le moins occupé : en général, ils ne prennent malheureusement en compte que les autres équipements WiFi.

Les axes d'amélioration

Si la communication reste médiocre malgré les efforts pour identifier et réduire à la source les interférences, on peut toujours essayer d'augmenter la puissance des émetteurs ou utiliser des antennes directionnelles afin d'augmenter le RSB (dans la limite légale, bien entendu). Malheureusement, si l'on a déployé plusieurs antennes, ceci peut provoquer encore plus d'interférences !

Autrement, il peut être intéressant de diminuer la taille des paquets WiFi transmis (fragmentation), de telle sorte qu'ils soient moins nombreux (en proportion) à contenir des bits erronés : cela n'améliorera pas le BER mais le FER deviendra moins mauvais. Il faut trouver un bon compromis car chaque paquet contient un en-tête d'une taille fixe, donc en multipliant les paquets on augmente également le volume total de données transmises. En outre, le risque de collisions augmente avec le nombre de paquets transmis.

On peut aussi diminuer le RTS *Threshold* et trouver sa valeur idéale : rappelons qu'il s'agit de la taille de paquet à partir de laquelle un paquet RTS (demande de parole) est envoyé avant l'émission du paquet de données (voir le chapitre 3, § 3.2.1).

On peut également installer des filtres radio sur le câble d'antenne, pour éliminer les interférences provenant d'autres canaux que celui qui a été choisi.

Il faut bien sûr s'assurer que l'adaptateur ait une bonne tolérance au bruit. Les produits sont en effet plus ou moins tolérants : ce paramètre doit vous être indiqué par le vendeur. Pour observer un FER inférieur à 1 % (moins d'un paquet sur 100 est perdu) à un débit de 1 Mb/s, un adaptateur classique requiert un RSB minimum de 4 dB.

Dans une connexion de point à point, une autre option consiste à installer un AP répétiteur entre les deux points à relier. Le RSB entre chaque point sera meilleur car la distance sera plus faible donc la puissance du signal plus forte. Le problème de cette solution est que le débit est au minimum divisé par deux par un répétiteur classique, comme nous l'avons vu au chapitre 4 (§ 4.2.2)... sauf si le répétiteur a deux circuits radio, permettant de retransmettre les paquets reçus sur un autre canal.

5.2.2 L'absorption et la réflexion

Lorsqu'un obstacle se situe entre l'émetteur et le récepteur, les ondes radio sont en partie reflétées et en partie (ou en totalité) absorbées par l'obstacle. La portion du signal qui parvient à traverser l'obstacle est donc affaiblie.

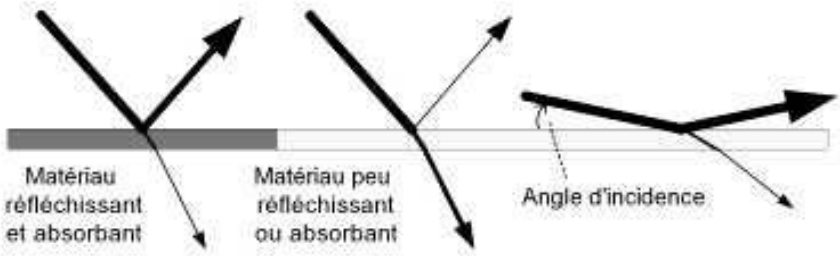


Figure 5.4 — Absorption et réflexion.

Fréquence et angle d'incidence

Plus la fréquence de l'onde radio est élevée, moins celle-ci traverse les obstacles. Le 802.11a et le 802.11n à 5 GHz, sont donc moins « pénétrants » que le 802.11b, le 802.11g ou le 802.11n qui reposent sur le 2,4 GHz.

Par ailleurs, plus l'angle d'attaque (également appelé l'angle « d'incidence ») est proche de la perpendiculaire, plus le signal traverse l'obstacle. Pour qu'une onde traverse une vitre, il vaudra mieux que l'angle soit proche de la perpendiculaire plutôt qu'en biais, sinon une partie importante de l'onde risque d'être réfléchie.

Le matériau

L'absorption et la réflexion dépendent naturellement de l'épaisseur de l'obstacle et du matériau dont il est constitué : bois, béton, métal, plastique, verre, eau ou autres. À titre indicatif, le béton et le métal absorbent davantage le signal que le plastique ou le verre. Un mur de 50 cm de béton est suffisant pour absorber la majeure partie du signal WiFi, alors que plusieurs façades successives en plastique laisseront en général passer une bonne partie du signal.

Un point important : l'eau absorbe très nettement les ondes à 2,4 GHz, c'est d'ailleurs la raison pour laquelle ces ondes sont utilisées dans les fours à micro-ondes pour chauffer les aliments. La première conséquence de cette observation est le fait qu'une liaison WiFi à l'extérieur est assez sensible à la météo ! Un jour de pluie ou de brouillard, la connexion risque d'être interrompue ou perturbée. De même, le bois, selon sa teneur en eau, arrêtera plus ou moins le signal.

Pour finir, les êtres humains, qui sont constitués en grande partie d'eau, absorbent une partie importante du signal WiFi ! Si l'on installe un réseau WiFi pour une grande salle de conférence, il faudra prendre en compte le fait que la connexion sera nettement moins bonne lorsque la salle sera pleine de monde. Pour limiter ce problème, une solution simple consiste à placer l'antenne en hauteur. En outre, si l'on peut positionner les utilisateurs de telle sorte qu'ils ne soient pas entre leur ordinateur et l'AP, on améliorera nettement la réception.

L'homme étant constitué en grande proportion d'eau, il atténue beaucoup le signal WiFi à 2,4 GHz. Il est donc préférable d'installer les antennes en hauteur. Voir également les questions de santé au chapitre 11.

Modélisation ou mesure

On pourrait essayer de modéliser quelle serait la couverture radio d'un site en fonction du plan des locaux, de la nature des murs, et ainsi de suite, afin de savoir où positionner un AP, mais la complexité des calculs est telle qu'il est préférable de simplement faire un test en conditions réelles à l'aide d'outils de mesure (voir paragraphes suivants). On peut ainsi connaître précisément la puissance du signal qui parvient à atteindre le récepteur et l'on peut également voir si le RSB est suffisant pour établir une connexion satisfaisante.

Il existe toutefois des logiciels de modélisation qui simulent le rayonnement électromagnétique dans un modèle de la zone étudiée en deux ou trois dimensions. Le prix très élevé de ces logiciels et le temps nécessaire à la réalisation d'une modélisation[1] ne justifient pas, en général, leur utilisation dans un contexte de réseau WiFi d'entreprise (et encore moins pour un particulier). Ils sont en revanche très appréciés, par exemple, pour positionner au mieux des antennes GSM dont le déploiement est très coûteux. Ceci dit, ils ne permettent pas de s'affranchir des tests sur le terrain.

5.2.3 La polarisation

Comme nous l'avons vu, au chapitre 4 (§ 4.4.1), les antennes WiFi entraînent une polarisation du signal qui peut être horizontale, verticale, selon un axe incliné, ou encore circulaire droite ou gauche (dans le sens des aiguilles d'une montre ou non).

Si l'axe de polarisation est vertical du côté de l'émetteur, il faudra qu'il soit également vertical pour le récepteur, sinon le signal sera atténué. Si les axes sont perpendiculaires le signal sera en grande partie voire complètement éliminé. De même, si la polarisation est circulaire droite pour l'émetteur (avec une antenne hélicoïdale), il faudra que le récepteur ait une polarisation circulaire gauche.

Dans la pratique, les réflexions et les diffractions peuvent modifier plus ou moins l'axe de polarisation du signal, donc le plus sûr consiste à régler l'inclinaison des antennes avec précision en utilisant un analyseur de signal.

Dans le cas de la polarisation circulaire, après une réflexion, la polarisation droite devient gauche et *vice versa*. Pour vous en convaincre, regardez un tire-bouchon dans un miroir : il ne tourne pas dans le même sens ! Ceci peut être utile pour limiter l'effet des réflexions : en effet, toutes les ondes atteignant l'antenne de réception après une réflexion, ou un nombre impair de réflexions, seront très atténuées.

1. Plus que le temps de calcul, il s'agit du temps qu'il faut à l'utilisateur pour configurer le logiciel avec un modèle précis du site.

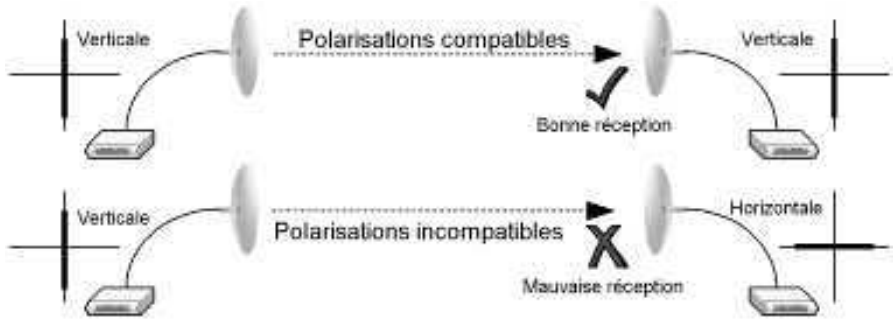


Figure 5.5 — Polarisation de l'antenne de l'émetteur et du récepteur.

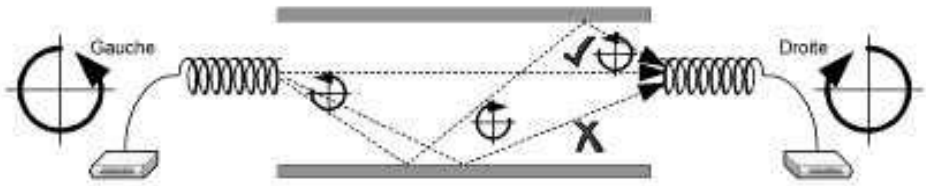


Figure 5.6 — Polarisation circulaire et réflexions.

En outre, les ondes ne se propagent pas de la même manière selon leur polarisation. Par exemple, pour une liaison à longue distance, la polarisation verticale est moins atténuée que la polarisation horizontale.

5.2.4 La diffraction

Le principe de Huygens-Fresnel

Un autre phénomène auquel les ondes radio sont sujettes est la diffraction. Elle peut être expliquée brièvement par le principe de Huygens-Fresnel : chaque point par lequel passe une onde peut être considéré comme une nouvelle source de l'onde, émise dans toutes les directions. En l'absence d'obstacles, la somme des ondes émises donne un front d'onde qui se propage « normalement », dans une direction, car les ondes émises dans les autres directions s'annulent mutuellement. Toutefois, dès que le front de l'onde se heurte à un obstacle, les ondes émises par les points situés aux extrémités de cet obstacle se propagent dans toutes les directions et ne sont plus annulées par les ondes voisines : l'obstacle peut ainsi être contourné, en particulier si ses bords sont saillants (fig. 5.7).

Pour vous en convaincre, la prochaine fois que vous prendrez un bain, essayez l'expérience suivante : restez immobile pour que la surface de l'eau soit lisse, puis placez votre bras gauche à l'horizontale, à moitié dans l'eau et tapotez l'eau avec votre main droite, à quelques dizaines de centimètres du bras gauche pour créer des

vaguelettes : vous constaterez que lorsque le front d'ondes atteindra votre bras, les ondes le contourneront, en s'atténuant un peu.

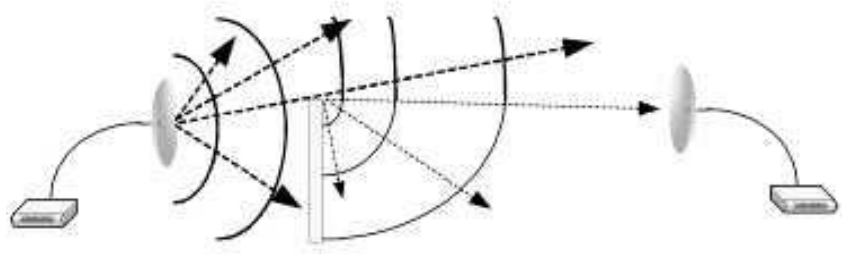


Figure 5.7 — La diffraction.

Calculer l'atténuation

Le signal diffracté subit tout de même une atténuation assez forte.

Le calcul théorique de cette atténuation peut être très complexe selon la forme de l'obstacle et la position relative des stations, donc nous nous limiterons à un exemple assez simple : deux stations utilisant le 802.11b, donc à 2,4 GHz, sont situées de part et d'autre d'un mur.

La première se trouve à une distance d_1 = 100 mètres du mur et la seconde à une distance d_2 = 200 mètres. Le mur est haut de h = 3 mètres (fig. 5.8).

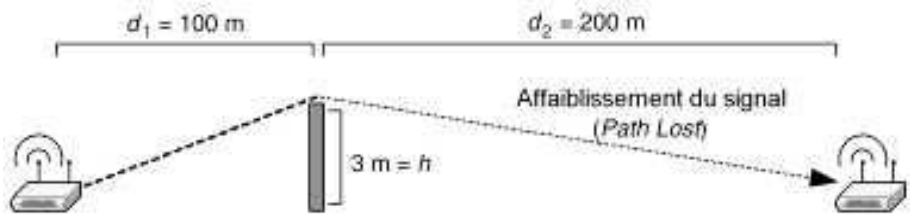


Figure 5.8 — Exemple de diffraction simple.

Le calcul de l'atténuation du signal commence par l'évaluation du facteur de Fresnel υ grâce à la formule suivante :

$$\upsilon = h \times \sqrt{2 \times \left(\frac{d_1 + d_2}{\lambda \times d_1 \times d_2} \right)}$$

λ est la longueur d'onde, égale à 0,125 mètre puisqu'on utilise le 802.11b.

Dans notre cas, on trouve environ $v = 1{,}47$. On peut maintenant calculer la perte approximative due à la diffraction, notée *PL* (*Path Loss*), grâce à la formule suivante :

$$PL = 20 \times \log\left(\frac{0{,}225}{v}\right)$$

On trouve une perte d'environ −16,3 dB, à intégrer dans le bilan radio. Cette formule est déduite d'un ensemble de formules beaucoup plus complexes, d'où le facteur 0,225 qui peut paraître tout à fait arbitraire. En outre, ce calcul n'est valable que si h est très petit par rapport à d_1 et d_2. En revanche, il est toujours valable dans les deux sens, quelle que soit la station émettrice ou réceptrice.

Notons pour finir que les phénomènes de diffraction sont d'autant plus importants que la longueur d'onde est grande (donc la fréquence faible) : il y a donc plus de diffraction pour les fréquences de 2,4 GHz que pour les fréquences de 5 GHz : le 802.11b et le 802.11g contournent donc mieux les obstacles que le 802.11a.

5.2.5 Les chemins multiples (multipath)

Le NLOS

Réflexions et diffractions sont utiles pour capter le signal à un endroit où l'émetteur n'est pas visible : on dit qu'on est en condition de *Non Line of Sight* (NLOS), c'est-à-dire que l'on n'a pas une ligne de vision directe. Mais les réflexions et diffractions peuvent également être nuisibles lorsqu'elles font apparaître de multiples chemins possibles entre l'émetteur et le récepteur (on parle de *multipath*). Dans ce cas, un même signal peut alors atteindre le récepteur à plusieurs moments différents. Il y a alors trois conséquences néfastes possibles (fig. 5.9) :

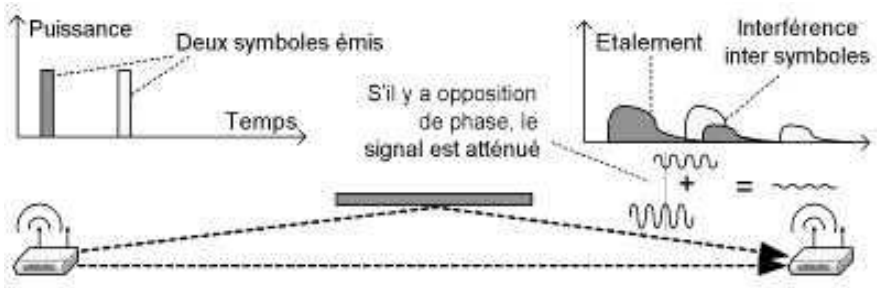


Figure 5.9 — Les conséquences du multipath.

1. si le décalage dans le temps est tel que les différentes ondes soient en opposition de phase, le signal est atténué, voire même complètement annulé si les ondes opposées ont une puissance identique ;
2. en arrivant par plusieurs chemins distincts, le signal est étalé dans le temps et le récepteur doit être capable de l'interpréter correctement ;

3. si le décalage est très important, un symbole peut arriver en même temps que le symbole suivant (interférence intersymboles ou ISI, voir le chapitre 2), ce qui perturbe fortement la communication.

Éviter les obstacles

Pour réduire les problèmes de réception en condition NLOS, on peut commencer par attaquer le mal à la racine en essayant de positionner les antennes et si possible les obstacles de telle sorte que les interférences soient moins intenses. Un outil d'analyse s'avère alors encore très utile : en déplaçant les antennes (ou les obstacles) et en mesurant l'impact sur le FER, la puissance du signal reçu et le RSB, on peut parvenir à améliorer la situation considérablement. Pour le problème d'opposition de phase, un déplacement des antennes ou des obstacles, même léger, peut parfois résoudre le problème : les interférences peuvent créer de petites zones d'ombres qu'on peut parfois simplement éviter.

On peut également veiller à limiter les surfaces réfléchissantes telles que les surfaces métalliques qui reflètent énormément le signal radio : il suffit parfois de relever les stores en métal pour obtenir un meilleur signal !

Agir sur les antennes

Un axe important d'amélioration consiste à choisir des antennes directionnelles plutôt qu'omnidirectionnelles et à les pointer dans la bonne direction, même si les stations sont proches et en vision directe.

En outre, on peut choisir d'installer des antennes hélicoïdales, car leur polarisation circulaire permet de limiter l'effet des réflexions comme nous l'avons vu plus haut.

Les réflexions peuvent aussi parfois provenir des antennes elles-mêmes, ou des câbles et connecteurs d'antenne s'ils sont mal conçus ou mal reliés : en particulier si leurs impédances (mesurées en Ohm, notées Ω) sont très différentes. Le plus simple est d'acheter les connecteurs et câbles conçus pour le type d'antenne que l'on souhaite installer.

Pour finir, certains adaptateurs mettent en œuvre des techniques de « diversité » (redondance) pour améliorer la réception et l'émission, en particulier en conditions de NLOS. La solution la plus répandue consiste simplement à utiliser deux antennes pour la réception, bien écartées l'une de l'autre. Grâce à cet espacement, on peut atténuer fortement les effets des interférences dues aux chemins multiples : en effet, si deux ondes s'annulent à l'arrivée sur l'une des deux antennes, il est peu probable qu'elles s'annuleront également à l'arrivée sur la deuxième antenne. Le récepteur percevra toujours au moins une partie du signal. C'est ce qu'on appelle la « diversité d'espace ».

Voyons pourquoi : si deux ondes issues du même émetteur s'annulent en un point, cela signifie qu'elles sont en opposition de phase, donc qu'elles ont suivi des parcours de longueurs différentes et que la différence entre ces longueurs est d'une demie longueur d'onde (ou encore de $1\,1/2$, $2\,1/2$, $3\,1/2$...).

Par exemple, à 2,4 GHz, la longueur d'onde est de 12,5 cm, donc la différence de parcours qui provoquera le plus d'interférences est de 6,25 cm. On aura le même

phénomène avec une différence de parcours de 18,75 cm, ou encore 31,25 cm, etc. Pour atteindre la deuxième antenne, les deux parcours ne seront pas les mêmes et il est peu probable que la différence de parcours provoque ici aussi une opposition de phase.

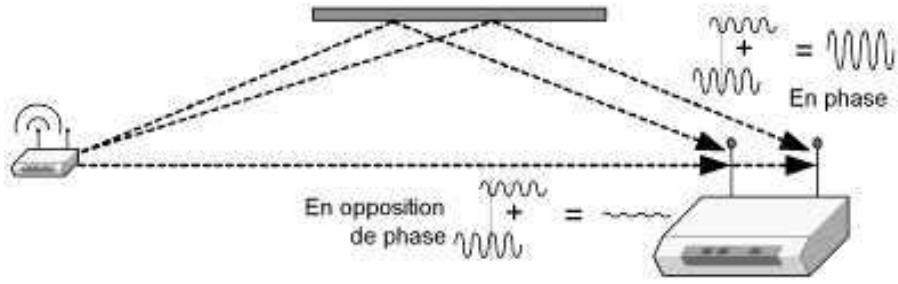


Figure 5.10 — La technique de diversité d'espace.

Bien choisir les adaptateurs

Une fois que l'on a fait le maximum pour régler le problème à la source, s'il subsiste des problèmes d'interférences, il reste quelques solutions : en premier lieu, on peut choisir des récepteurs sensibles, tolérants au bruit, mais aussi résistants à l'étalement du signal dans le temps (*delay spread*). Si un adaptateur indique qu'il peut gérer un étalement de 500 nanosecondes (ns) pour un débit de 1 Mb/s avec un FER inférieur à 1 %, alors cela signifie que la différence entre le temps de parcours du chemin le plus long et celui du chemin le plus court ne devra pas être supérieure à 500 ns, c'est-à-dire $5 \cdot 10^{-7}$ secondes. Puisque les ondes se déplacent dans l'air (quasiment) à la vitesse de la lumière ($3 \cdot 10^8$ m/s), on en déduit qu'avec cet adaptateur, la différence de distance de parcours doit rester inférieure à $3 \cdot 10^8 \times 5 \cdot 10^{-7} = 150$ mètres pour que la communication soit satisfaisante. Le même adaptateur indique une limite de *delay spread* de 65 ns pour le 11 Mb/s, soit une différence de parcours de 19,5 mètres seulement. Avec deux ou trois rebonds sur des surfaces très réfléchissantes, ou bien dans un grand hangar, cette limite peut vite être atteinte : les débits élevés sont donc bien plus sensibles aux interférences inter symboles (ISI) que les faibles débits.

Forcer le bas débit

Une autre solution consiste simplement à forcer les stations à communiquer moins vite. Si vous avez déjà assisté à un concert dans une salle dont la sonorisation laisse à désirer (avec de l'écho ou de la réverbération entraînant un son diffus), vous aurez peut-être remarqué que les morceaux les plus lents sont les plus agréables à écouter, alors que les morceaux rapides frôlent la cacophonie. De la même manière, si le *multipath* (qui n'est rien d'autre qu'un écho) pose problème, le fait de forcer les stations à communiquer moins vite permettra de diminuer les interférences et le taux de paquets erronés (FER). À ce sujet, l'indication de débit affichée par certains pilotes WiFi (en particulier le Zéro Config de Windows XP) peut être trompeuse : il s'agit du débit au niveau

physique, négocié automatiquement entre la station et l'AP, pas du débit réellement observé au niveau des couches réseaux supérieures. Si des paquets sont perdus suite aux problèmes de multipath, cela n'apparaît donc pas dans ce paramètre : on peut voir « 11 Mb/s » alors que tous les paquets émis sont corrompus et que la communication est impossible ! On obtiendra parfois un meilleur débit réel en forçant son ordinateur à négocier un débit plus bas (1, 2 ou 5,5 Mb/s).

Le 802.11g, le 802.11a et le 802.11n utilisent la modulation OFDM, comme nous l'avons vu au chapitre 2. L'OFDM est assez résistant au multipath car il utilise des symboles espacés dans le temps mais portant chacun, en contrepartie, une grande quantité d'information. Le 802.11g n'utilise l'OFDM que pour les débits les plus élevés (à partir de 6 Mb/s). Si l'on observe des problèmes d'interférences ISI aux débits les plus élevés avec le 802.11g, on est obligé de « redescendre » en DSSS, qui est moins adapté au multipath, ce qui implique souvent de descendre encore jusqu'à 5,5 Mb/s voire 2 Mb/s ou 1 Mb/s. En revanche, le 802.11a repose entièrement sur l'OFDM, quel que soit le débit utilisé, ce qui le rend globalement plus efficace dans le contexte NLOS (mais pas forcément à longue distance).

5.2.6 Les zones de Fresnel

La vision directe

L'idéal pour une connexion de point à point est que les deux stations soient en vision directe, ou *Line of Sight* (LOS), avec aussi peu d'interférences multipath que possible. Mais est-ce suffisant ? Cette idée de « vision directe » trahit le fait que l'on considère intuitivement les ondes radios comme des ondes lumineuses. Malheureusement, cette analogie est parfois trompeuse. En effet, la longueur d'onde des micro-ondes du WiFi est beaucoup plus longue que celle des ondes lumineuses : 12,5 cm pour le 2,4 GHz et 6,0 cm pour le 5 GHz contre 0,4 à 0,75 micromètre (μm) pour la lumière visible. Or, les phénomènes de diffraction sont beaucoup plus importants lorsque la longueur d'onde est importante, comme nous l'avons vu.

Ainsi, avec les ondes radio, la notion de « vision directe » est bien plus floue qu'avec la lumière visible : il ne suffit pas qu'il n'y ait aucun obstacle sur l'axe entre l'émetteur et le récepteur, il faut également qu'aucun obstacle ne se trouve *à proximité* de cet axe, sinon une partie importante de l'énergie du signal sera perdue ! Pour vous faire une idée de ce phénomène, imaginez s'il s'appliquait également aux ondes lumineuses : les nuages vous feraient de l'ombre avant même de cacher le soleil, le sol lui-même vous empêcherait de voir un objet lointain et il faudrait bien écarter tous les objets entre le canapé et la télévision pour pouvoir la regarder ! Mais comment évaluer le dégagement minimal nécessaire ?

Le dégagement minimal

On peut considérer que l'énergie transmise de l'émetteur radio vers le récepteur se propage essentiellement au sein d'un ellipsoïde de révolution (c'est-à-dire en forme de ballon de rugby très allongé) : c'est ce qu'on appelle la « zone de Fresnel », délimitée par la « surface de Fresnel ». On devrait plutôt préciser *la première* zone de Fresnel

délimitée par *la première* surface de Fresnel, car il en existe une infinité, emboîtées les unes dans les autres comme des poupées russes. Le rayon de la $n^{ième}$ surface de Fresnel peut être calculé pour chaque point de l'axe émetteur/récepteur grâce à la formule suivante :

$$r_n = \sqrt{n \times \lambda \times \frac{d_1 \times d_2}{d_1 + d_2}}$$

λ est la longueur d'onde (0,125 mètre à 2,4 GHz, 0,06 mètre à 5 GHz) ;
d_1 est la distance de l'émetteur jusqu'au point de l'axe émetteur/récepteur pour lequel on cherche le rayon de l'ellipsoïde ;
d_2 est la distance du récepteur à ce même point.

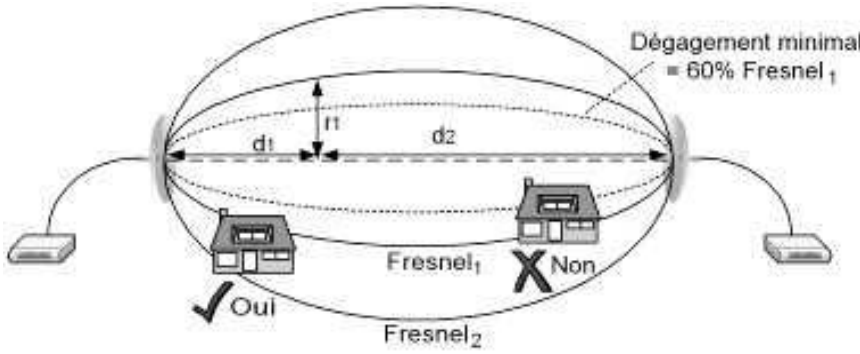


Figure 5.11 — Les ellipsoïdes de Fresnel et le dégagement minimal.

Puisque l'essentiel de l'énergie du signal est diffusé dans la première zone de Fresnel, il faut éviter tout obstacle au cœur de cette zone. Dans la pratique, il est suffisant de dégager au moins 60 % de cette zone (au centre) pour avoir une bonne réception. On obtient donc le dégagement minimal d_{min}, en tout point de l'axe entre l'émetteur et le récepteur, par la formule suivante :

$$d_{\min} = 60\ \% \times \sqrt{\lambda \times \frac{d_1 \times d_2}{d_1 + d_2}}$$

Par exemple, si deux stations sont distantes de 1 000 mètres et qu'un obstacle se situe non loin d'un point de l'axe situé à 300 mètres de l'émetteur, on peut calculer la distance minimale entre ce point de l'axe et l'obstacle :

$$d_{\min} = 60\ \% \times \sqrt{0{,}125 \times \frac{700 \times 300}{700 + 300}} \cong 3{,}07\ m$$

Il faut donc s'assurer que l'obstacle soit bien à plus de 3 mètres de l'axe entre l'émetteur et le récepteur, sinon une partie importante du signal sera perdue. Par exemple, si la moitié de la zone de Fresnel est obstruée par un obstacle, alors plus de 75 % de la puissance du signal est perdue ! Cela correspond à une perte de 6 dB, ce qui est énorme car le signal porte alors deux fois moins loin.

La hauteur minimale

Bien entendu, le sol lui-même est un obstacle, donc il faut faire le calcul pour chaque point où le sol est susceptible d'être dans la zone « interdite ». Si le sol est plat et que les antennes sont toutes deux à la même hauteur, alors le point pour lequel il faut faire le calcul est à mi-chemin entre l'émetteur et le récepteur, là où l'ellipsoïde est le plus large. À partir de la formule précédente, on trouve la hauteur minimale à laquelle il faut installer deux antennes pointées l'une vers l'autre sur un terrain plat :

$$h_{\min} = 30\ \% \times \sqrt{\lambda \times d}$$

d est la distance entre les stations.

Dans notre exemple, les stations sont à une distance d = 1 000 mètres l'une de l'autre donc on calcule qu'elles doivent être installées au moins à 3,35 mètres de hauteur (idéalement sur un mât ou sur le toit d'un bâtiment).

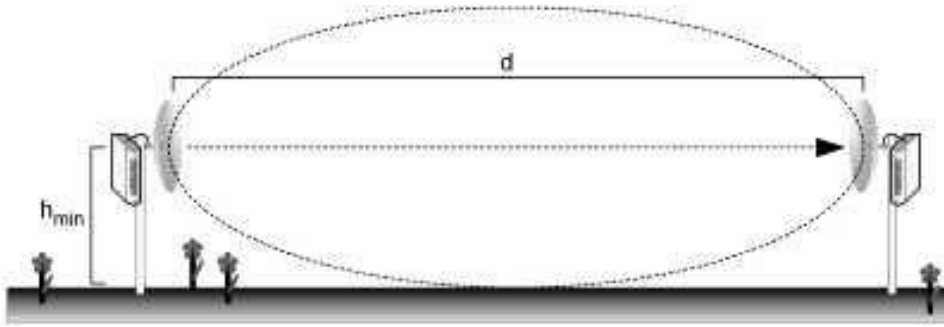


Figure 5.12 — La hauteur minimale pour une connexion de point à point.

Les surfaces réfléchissantes

Les surfaces de Fresnel sont définies de la façon suivante : si une onde part de l'émetteur (point A) vers un point M de la $n^{\text{ième}}$ surface de Fresnel, puis vers le récepteur (point B), alors on a :

$$AM + MB - AB = n \times \lambda/2$$

En d'autres termes, la différence de parcours entre la ligne droite et le passage par un point d'une surface de Fresnel est un multiple de la moitié de la longueur d'onde.

Par conséquent, si une surface réfléchissante est tangente à la première surface de Fresnel, alors les ondes réfléchies arriveront au récepteur en opposition de phase par rapport au signal parti en ligne droite, ce qui diminuera l'intensité du signal reçu. On peut donc dire que la première surface de Fresnel, ainsi que toutes les surfaces impaires, sont « destructives ». À l'inverse, si une onde est réfléchie au niveau de la deuxième surface de Fresnel, elle arrivera en phase avec l'onde directe et amplifiera le signal. Les surfaces de Fresnel paires sont donc « constructives ».

Par exemple, si deux antennes sont placées de part et d'autre d'un terrain plat (tel qu'un lac), à 1 000 mètres l'une de l'autre et à la même hauteur, il faudra faire attention à ne pas les placer à une hauteur telle que le lac soit tangent à une surface impaire de Fresnel. Puisque le lac est horizontal et que les antennes sont à la même hauteur, les réflexions qui pourraient être gênantes auraient lieu à mi-chemin. Grâce aux formules précédentes, on calcule le rayon des quatre premières surfaces de Fresnel à mi-chemin entre les antennes et l'on trouve :

$$r_1 = 5{,}59 \text{ m}, r_2 = 7{,}90 \text{ m}, r_3 = 9{,}68 \text{ m}, r_4 = 11{,}18 \text{ m}.$$

On a vu plus haut que sur terrain plat, à 1 000 mètres de distance, il faut placer les antennes au minimum à 3,35 mètres du sol. On sait maintenant qu'il faut également éviter de les placer à près de 5,59 m, ou 9,68 m, mais plutôt, si possible, à 7,9 m ou 11,18 m (ou sinon, simplement à 3,35 m).

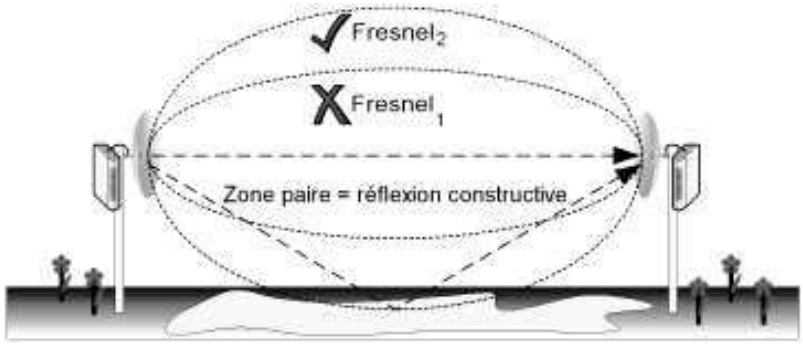


Figure 5.13 — Réflexions constructives ou destructives.

5.2.7 La disponibilité d'une liaison point à point

Lorsque l'on met en place une liaison radio de point à point d'une qualité professionnelle, il est nécessaire que le débit soit très stable et plus généralement que la disponibilité du lien soit permanente. Avec le WiFi, il est impossible de garantir une fiabilité à 100 %, car il repose sur des fréquences libres : n'importe qui peut rajouter un nouveau réseau à proximité à tout moment et perturber ainsi votre liaison point à point.

Il existe une multitude de modèles permettant d'estimer *a priori* quelle sera la disponibilité d'une connexion radio en fonction de multiples paramètres. Citons à titre d'exemple le modèle de W. T. Barnett pour les communications à l'aide des micro-ondes[1]. Ce modèle a été conçu pour les ondes de 4 et 6 GHz sous licence, donc il ne doit servir que de première approximation pour une liaison WiFi et nous ne le présentons ici que pour donner une idée des influences relatives des facteurs de l'environnement.

1. *Engineering Considerations for Microwave Communications Systems*.

Dans ce modèle, la disponibilité D de la liaison, c'est-à-dire le pourcentage du temps pendant laquelle elle est satisfaisante, est estimé grâce à la formule suivante (ramenée au système métrique par rapport à la formule originale) :

$$D = 1 - a \times b \times f \times d^3 \times 10^{-\frac{M}{10}} \times 10^{-5}$$

a est le facteur de rudesse du relief. De 0,25 pour un relief très escarpé à 4 pour une surface lisse telle qu'un lac ;
b est le facteur de climat. De 0,125 pour un endroit très sec à 0,5 pour une région humide ;
f est la fréquence en gigahertz (GHz) ;
d est la distance entre les deux antennes, en kilomètres (km) ;
M est la marge de la liaison, en décibels (dB), tels que nous l'avons calculée plus haut, c'est-à-dire la somme de tous les gains (l'émetteur et les deux antennes), plus toutes les pertes (l'affaiblissement en espace libre et la perte dans les câbles), moins la sensibilité du récepteur (les pertes et la sensibilité ayant des valeurs négatives).

En choisissant des paramètres arbitraires, vous trouverez sans doute des valeurs supérieures à 99,99 %. Ce n'est pas une erreur de calcul : une liaison ayant une disponibilité de 99 % est loin d'être excellente car cela signifie qu'elle sera indisponible 1 % du temps, soit près d'un quart d'heure par jour et plus de 87 heures par an ! Cela suffit pour un usage personnel, mais pas pour une connexion professionnelle.

5.3 DÉPLOYER DE MULTIPLES AP

Maintenant que les ondes radio n'ont plus de secrets pour vous, nous allons aborder le cas du déploiement au sein des locaux d'une entreprise. Dans ce contexte, l'emploi de multiples AP est souvent obligatoire pour obtenir à la fois :

- une bonne couverture radio et éviter ainsi les zones d'ombre ;
- une bonne capacité, c'est-à-dire un débit suffisant pour chaque employé, en fonction des applications prévues.

5.3.1 La densité d'AP et le débit

Nous avons vu, au chapitre 2 (§ 2.2.2), que plus on s'éloigne d'un AP, plus le débit diminue : l'AP et la station négocient régulièrement le débit de leurs échanges en fonction de la qualité du lien radio. La figure 2.5 indique le débit théorique (c'est-à-dire au niveau de la couche physique) en fonction de la distance, selon qu'on utilise le 802.11a, le 802.11b ou le 802.11g, en intérieur ou en extérieur. Ces chiffres théoriques sont présentés à titre indicatif : dans la pratique le débit et la portée réels pourront varier considérablement d'un site à l'autre et ils seront généralement beaucoup plus faibles.

Admettons que l'on choisisse d'installer des AP 802.11g dans les locaux de l'entreprise et que l'on souhaite pouvoir profiter d'un débit supérieur à 9 Mb/s en tout point. La figure 2.5 nous indique qu'il faut alors qu'on soit toujours à moins de 20 mètres d'un AP. Les AP doivent donc être espacés de 40 mètres au maximum. De même, si l'on souhaite un débit minimal de 36 Mb/s, il faut espacer les AP de 20 mètres seulement ! On constate que plus le débit souhaité est élevé, plus la densité d'AP doit être importante.

À moins que la configuration des bureaux ne l'interdise, on déploie typiquement les AP en un maillage plus ou moins hexagonal (comme les cellules d'une ruche d'abeilles). Cette configuration permet de déployer un minimum d'AP tout en respectant la contrainte de densité pour obtenir un débit satisfaisant en tout point (fig. 5.14).

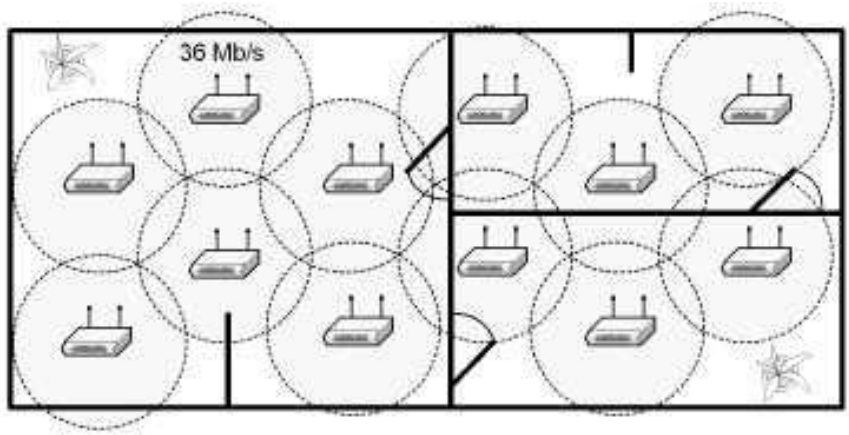


Figure 5.14 — Densité de points d'accès et débit.

5.3.2 Limiter les interférences entre AP

Espacer les canaux identiques

Chaque AP est configuré pour utiliser un canal donné. Afin de limiter les interférences entre les AP, il est nécessaire d'écarter autant que possible ceux qui utilisent un même canal. Une confusion fréquente consiste à penser qu'il faut utiliser le même canal pour tous les AP d'un même réseau sans fil : bien au contraire, il faut varier les canaux afin que chaque cellule n'interfère pas avec les cellules voisines. Seul le SSID devra être le même si l'on veut permettre aux utilisateurs de passer d'une cellule à une autre sans rupture de connexion.

Avec le 802.11b, le 802.11g et le 802.11n à 2,4 GHz, on dispose de treize canaux en France, mais comme vous le savez, les canaux voisins se superposent de sorte que seuls trois canaux indépendants peuvent être utilisés au même endroit. On choisit en général les canaux 1, 6 et 11. Le schéma suivant montre à quoi doit ressembler notre déploiement pour limiter les interférences entre les AP.

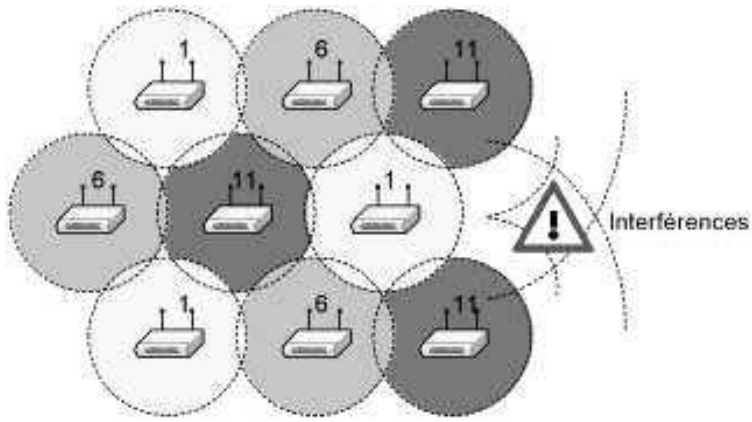


Figure 5.15 — Interférences entre les AP avec le 802.11b ou le 802.11g.

On constate qu'avec seulement trois canaux indépendants, il n'est pas possible d'espacer beaucoup les AP utilisant le même canal : en général, une seule cellule les sépare. De ce fait, on ne peut jamais éviter complètement les interférences. Plus la densité des AP est importante, plus ces interférences sont perceptibles et diminuent le débit. Par exemple, nous avons vu plus haut que pour pouvoir offrir un débit de 36 Mb/s en tout point avec le 802.11g, il fallait espacer les AP tout au plus de 20 mètres : cela signifie que deux AP utilisant le même canal seront au maximum espacées de 40 mètres. Les interférences seront telles que l'on n'obtiendra jamais les 36 Mb/s souhaités !

> Avec le 802.11b et le 802.11g, il est difficile d'avoir une couverture uniforme permettant d'atteindre en tout point le débit maximal.

Limiter le recouvrement des cellules

Un premier axe d'amélioration consiste à utiliser des antennes directionnelles ou sectorielles pour concentrer le signal vers la zone à couvrir, en essayant d'éviter le débordement vers les cellules voisines. En complément, si l'AP le permet, on peut également diminuer la puissance du signal émis. Il faut toutefois s'assurer que la couverture dans la cellule ne soit pas détériorée.

En outre, une station associée à un AP émet sur le canal défini par cet AP. Résultat, si un AP autorise des stations éloignées à s'associer à lui, ces stations seront des sources d'interférences pour les autres AP utilisant le même canal. Ainsi, il peut être intéressant de diminuer la sensibilité de l'AP pour empêcher des stations distantes de s'y associer : elles choisiront automatiquement un AP plus proche d'elles. Si l'AP n'offre pas l'option de réduire sa sensibilité, on peut également utiliser un câble d'antenne à forte perte : cela reviendra à perdre simultanément de la sensibilité et de la puissance d'émission, donc à réduire le rayon de la cellule. C'est une moins bonne solution car la perte est à la fois à la réception et à l'émission : il faut à nouveau faire attention à ne pas détériorer la couverture au sein de la cellule.

Utiliser le 802.11a ou le 802.11n à 5 GHz

Dernière solution, sans doute la meilleure si l'on souhaite absolument avoir un réseau sans fil très performant : utiliser le 802.11a ou le 802.11n à 5 GHz. En effet, à 5 GHz, on dispose de 19 canaux indépendants. Ceci permet d'espacer bien davantage les AP utilisant un même canal et de limiter ainsi considérablement les interférences. La figure 5.16 montre à quoi ressemble un déploiement à 5 GHz. Remarquez la distance importante qui sépare deux AP utilisant le même canal.

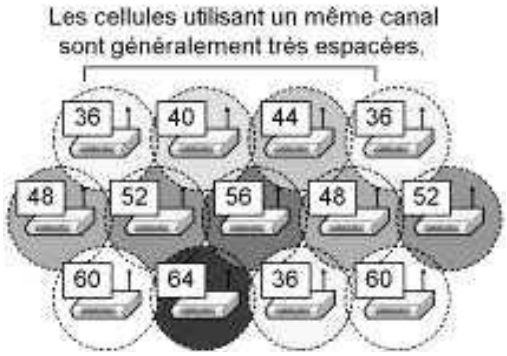


Figure 5.16 — Maillage dense à 5 GHz.

Un autre avantage considérable du WiFi à 5GHz est le fait que cette bande de fréquences est peu encombrée : on ne sera pas gêné par le Bluetooth, les fours à micro-ondes, les téléphones portables, etc. En outre, le WiFi à 5 GHz étant relativement peu répandu en France, contrairement au 802.11b au 802.11g et au 802.11n à 2,4 GHz, il est peu probable que le réseau sans fil de votre voisin sera en WiFi à 5 GHz : cela limite encore les possibilités d'interférences.

En termes de sécurité, le fait d'utiliser une technologie bien connue mais relativement peu répandue est sans doute un avantage : cela limite d'autant le nombre de curieux susceptibles de détecter votre réseau et de chercher à s'y introduire.

En revanche, le WiFi à 5 GHz n'a pas que des atouts : ses deux principaux inconvénients par rapport au WiFi à 2,4 GHz sont le prix et le consensus. En effet, les AP et les adaptateurs à 5 GHz sont en général légèrement plus chers que les équipements à 2,4 GHz. D'autre part, le 5 GHz est encore rare en entreprise et il l'est encore plus dans les *hotspots*. Il y a deux conséquences à cela : d'abord les produits disponibles sont moins nombreux car le marché est plus restreint. Il existe très peu d'ordinateurs portables vendus avec le WiFi à 5 GHz intégré. Ceci commence toutefois à changer. D'autre part, si vous optez exclusivement pour le 5 GHz, les adaptateurs de vos employés ne leur permettront pas de se connecter à la grande majorité des *hotspots*, ce qui est bien dommage car vous perdrez ainsi une partie de l'intérêt du WiFi : la possibilité pour vos employés de se connecter pendant leurs déplacements, dans des hôtels, des aéroports et tout autre lieu public.

Une bonne solution consiste à déployer un réseau à double radio, l'une en 802.11b/g et l'autre en 802.11n à 5 GHz, et d'équiper les employés avec des adaptateurs

802.11a/b/g/n. Ils pourront ainsi se connecter dans tous les *hotspots*, utiliser le WiFi chez eux avec un routeur WiFi bas de gamme, tout en profitant d'une excellente connexion WiFi en 802.11n à 5 GHz au bureau.

Les déploiements en « trois dimensions »

Lorsque l'on déploie un réseau sans fil sur plusieurs étages d'un même bâtiment, il faut prendre garde aux interférences qui peuvent provenir des AP des étages voisins. Le problème du positionnement des AP devient assez complexe lorsque l'on rajoute cette troisième dimension verticale. Une façon de procéder est de placer les AP de la même manière que les oranges dans un étalage d'épicerie : on commence par disposer les AP en un maillage hexagonal au 1er étage, puis on place les AP du 2e étage en un maillage hexagonal décalé par rapport à celui du 1er étage de sorte qu'aucun AP ne soit à la verticale directe d'un autre AP. Et ainsi de suite pour chaque étage.

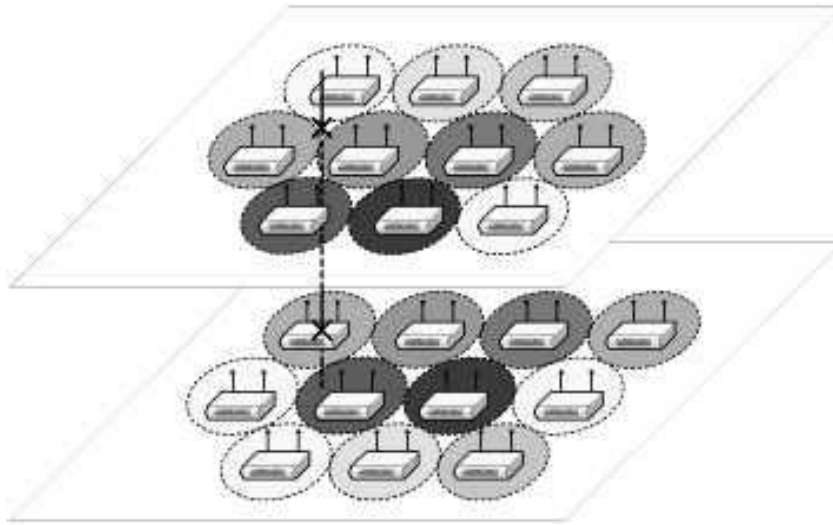


Figure 5.17 — Déploiement en trois dimensions.

Comme on peut le voir, un déploiement en 3D avec seulement trois canaux est presque irréalisable sans interférences. Dans ce contexte, l'avantage du 5 GHz est très important car on dispose de plus de canaux pour éviter les interférences. Quoi qu'il en soit, on peut améliorer la situation en utilisant des antennes intégrées aux faux plafonds : elles ont l'avantage de rayonner relativement peu vers le haut, donc de limiter le débordement à l'étage supérieur.

5.3.3 Les réseaux sans fil à haute capacité

Capacité souhaitée et densité d'AP

Chaque AP est limitée en capacité par la technologie employée : 11 Mb/s pour le 802.11b (et plutôt 5 à 6 Mb/s réels), 54 Mb/s pour le 802.11g (22 à 25 Mb/s réels),

54 Mb/s pour le 802.11a (25 à 27 Mb/s réels) et 300 Mb/s pour le 802.11n (120 à 150 réels) si l'on agrège deux canaux voisins. Même si le rayonnement radio d'un unique AP permet de couvrir l'ensemble des bureaux de l'entreprise, il sera sans doute nécessaire de mettre en place plusieurs AP pour permettre à chaque utilisateur de profiter d'une connexion satisfaisante.

L'objectif que vous vous fixerez pour la capacité de votre réseau sans fil impactera donc fortement le déploiement. Voici deux cas extrêmes :

- Vous ne prévoyez que quelques utilisateurs occasionnels et peu exigeants en bande passante : simple surf sur Internet ou consultation d'e-mails. La majorité des employés passera en général par le réseau filaire pour accéder au réseau local ou à Internet.
- Vous prévoyez au contraire que la majorité des employés utilisera exclusivement le WiFi pour accéder au réseau d'entreprise. Ils téléchargeront des fichiers volumineux, assisteront à des vidéoconférences, téléphoneront en voix sur IP en passant par le réseau sans fil, ce qu'on appelle le *Voice over Wireless IP* (VoWIP).

Si le réseau sans fil doit servir exclusivement à se connecter à Internet et que la connexion à Internet est une simple ligne ADSL à 1 Mb/s, alors cette connexion ADSL sera saturée bien avant le réseau WiFi (en tout cas si la couverture radio est correcte) car sa bande passante est plus faible que celle d'un AP. Pour vous en convaincre, imaginez un gros tuyau connecté à un petit tuyau : le débit possible est déterminé uniquement par le plus petit tuyau, c'est-à-dire par le goulot d'étranglement. Si vous préférez, imaginez une autoroute débouchant sur une petite route communale. Il faut bien sûr se demander si la situation ne risque pas de changer à court ou moyen terme : est-il possible que le réseau sans fil serve un jour à accéder au réseau local ? Prévoyez-vous de passer à plus ou moins court terme à une connexion à Internet à très haut débit, par exemple via une fibre optique ?

Si vous estimez que la capacité du réseau sans fil ne sera pas limitante, alors le déploiement radio se résume uniquement à un problème de couverture radio, c'est-à-dire à éviter les zones d'ombre et les interférences, en offrant en tout point un niveau de réception supérieur à un seuil que l'on s'est fixé, comme nous l'avons vu plus haut.

Dans le cas contraire, le WiFi à 5 GHz s'impose car il n'est pas possible de déployer une haute densité d'AP en WiFi à 2,4 GHz sans avoir beaucoup d'interférences. Il faut essayer de trouver la densité d'AP nécessaire pour satisfaire les besoins des utilisateurs. Ce n'est pas une chose facile et aucune méthode ne peut être généralisée à tous les contextes. Le plus sûr est d'analyser attentivement le trafic réseau existant sur votre réseau filaire et de vous calquer sur ce trafic pour trouver la densité d'AP nécessaire.

Débit minimal par service

En fonction des applications prévues, vous pouvez essayer d'évaluer le débit minimal que vous souhaitez offrir à chaque utilisateur. Par exemple, pour une simple navigation sur Internet, on peut estimer que 56 kb/s est un minimum absolu : c'est la vitesse d'une connexion à bas débit par une ligne téléphonique. Certains estimeront que naviguer sur Internet est insupportable en dessous de 512 kb/s, vitesse d'une ancienne

connexion ADSL d'entrée de gamme. Ces critères sont très subjectifs et dépendent entièrement de votre contexte. Dans le cas de la simple navigation sur Internet, il faut également considérer le taux d'utilisation moyen de la bande passante. En effet, même un utilisateur surfant activement sur Internet ne change pas de page en permanence. Il prend le temps de lire la page actuelle avant de passer à la suivante. Un taux d'utilisation moyen pour le simple surf sur Internet est souvent inférieur à 10 % ! Ainsi, avec une bande passante égale à 1 Mb/s, il est en général possible d'avoir 20 personnes surfant simultanément sur Internet, chacune ayant l'impression de profiter seule d'une ligne à 512 kb/s. En revanche, dès qu'une personne lance un téléchargement sur Internet, son taux d'utilisation passe à 100 % et tout le monde en pâtit.

Pour certains services, il existe des limites assez bien définies : par exemple, pour la voix sur IP, la limite de débit en dessous de laquelle on subira une détérioration très nette de la qualité de la communication est souvent indiquée par la documentation du produit utilisé. Par exemple, Skype affirme utiliser de 3 à 16 kb/s pendant une communication. D'autres systèmes de VoIP pourront utiliser plus de 30 à 50 kb/s. Le *streaming vidéo* et les vidéoconférences sont très gourmands en bande passante : selon la qualité de l'image et la fluidité de l'animation, il faut compter entre environ 30 kb/s et 400 kb/s et jusqu'à plus d'1 Mb/s pour une très bonne qualité d'image et de son !

L'accès aux ressources du réseau local (serveurs de fichiers, base de données, Intranet, postes des autres utilisateurs…) peut rapidement consommer toute la bande passante disponible : par exemple, si un employé décide d'enregistrer une copie de son disque dur de 100 Go sur le serveur de sauvegardes, il saturera sans doute complètement l'AP auquel il est associé et ce pendant plusieurs heures.

Si l'on souhaite éviter cela et plus généralement pour mieux contrôler le trafic réseau, il est nécessaire de mettre en œuvre des équipements (AP, commutateurs, routeurs ou serveurs) capables de limiter la bande passante par utilisateur ou par type de trafic. Nous avons vu, au chapitre 3 (§ 3.2.3), que les produits WMM offrent une solution à ce problème en différenciant les classes de trafic (TC) et en leur affectant des priorités variées. On peut par exemple décider de réserver au moins 50 % de la bande passante à la VoWIP, ou encore restreindre le débit par utilisateur à 1 Mb/s au maximum.

Utilisation maximale du réseau sans fil

Dans un deuxième temps, il faut chercher à évaluer quelle sera l'utilisation maximale du réseau sans fil, tous utilisateurs confondus. Pour cela, il faut imaginer le pire scénario que l'on accepte de gérer. Il est évident que si tous les employés se mettent d'accord pour saturer le réseau, ils parviendront sans doute à leur fin, mais ce scénario est à exclure : il faut chercher le pire scénario dans un contexte « raisonnable »… encore un critère subjectif !

Par exemple, une société comptant 100 employés décide de mettre en œuvre un réseau WiFi en complément de son réseau filaire. On peut supposer que les employés prendront goût à la mobilité offerte par ce réseau sans fil et seront nombreux à s'y connecter. On peut donc imaginer que le pire scénario sera le suivant : 90 personnes

associées au réseau sans fil en même temps, dont 30 en train de surfer activement sur Internet, avec 20 téléchargements importants en cours et 30 utilisateurs en pleine discussion en VoWIP, plus un total de 20 téléchargements intensifs sur le réseau local. On part du principe que la connexion à Internet est très rapide et n'est pas un goulot d'étranglement. On arrive à une estimation de 60 Mb/s consommés au maximum, par exemple.

Répartition de la charge entre les AP

Attention : ce débit est un débit réel et non théorique. Sachant qu'au mieux, un AP 802.11a est capable d'offrir 25 Mb/s de débit réel, il faut donc un minimum de 3 AP pour atteindre la capacité souhaitée si l'on choisit de déployer en 802.11a. En supposant que les utilisateurs soient bien répartis équitablement entre les trois AP, on a 20 utilisateurs par AP, donc environ 19 Mb/s de débit réel par AP. On part ici du principe que la bande passante est simplement divisée entre les utilisateurs (comme des parts d'un gâteau), mais c'est faux : plus les utilisateurs sont nombreux, plus les collisions CSMA/CA (voir le chapitre 3, § 3.2.1) sont importantes, d'où des pertes de débit importantes (c'est un peu comme si l'on perdait une partie du gâteau à chaque fois que l'on en découpait une part). Il est donc plus raisonnable de tabler sur au moins quatre AP.

Admettons que les 100 employés soient répartis de façon homogène sur un étage de 32 mètres de longueur sur 24 mètres de large, soit 768 m^2. La densité moyenne d'employés est donc égale à environ 0,13 employé par mètre carré. Théoriquement, en installant un AP en plein centre des locaux, chaque employé sera à moins de 20 mètres de l'AP central, ce qui lui permettra, s'il est seul à se connecter, de profiter du débit maximal de l'AP, sauf obstacle ou interférence. Malheureusement, nous avons vu qu'avec le besoin de capacité que l'on a, un unique AP ne pourra pas fournir toute la bande passante nécessaire à tous les utilisateurs, simultanément : nous avons estimé qu'il en fallait quatre. Il reste donc à les positionner intelligemment et à régler leurs canaux correctement.

Simulations et tests

Une façon moins approximative d'estimer le nombre d'AP nécessaires pour supporter une certaine capacité avec un nombre d'utilisateurs donné est d'utiliser des simulateurs radio, mais ils sont très chers et longs à régler. On peut également utiliser le logiciel libre Network Simulator qui possède des fonctions de simulations de trafic réseau très poussées. Mais il n'est pas très simple à installer et à utiliser.

Enfin, un test en grandeur nature reste la façon la plus fiable de déterminer le nombre d'AP à installer. Puisqu'il est difficile de réunir assez de personnes pour faire un test de charge réaliste, une meilleure approche consiste à utiliser des générateurs de trafic réseau : c'est d'ailleurs l'une des nombreuses fonctions de Network Simulator.

5.3.4 L'audit de site

Pour savoir combien d'AP installer et où les placer, la solution la plus simple consiste à réaliser ce qu'on appelle un « audit de site » (*site survey*). Cela consiste à installer un ou plusieurs AP aux endroits qui paraissent les plus adaptés, puis à mesurer le signal en se déplaçant dans les locaux. Il n'est pas nécessaire de connecter les AP au réseau, mais simplement de les alimenter en électricité et de les allumer. Si l'on observe des zones d'ombre, des interférences ou encore un débit insuffisant, il faut déplacer les AP et recommencer. Bien que cela soit une solution assez « artisanale », elle est assez fiable pour s'assurer que la couverture radio soit bonne[1]. Les outils que l'on peut utiliser pour réaliser l'audit de site sont très nombreux. Nous allons commencer par les plus simples pour aboutir aux plus complets.

Outils des pilotes

Le plus simple consiste à se déplacer avec un ordinateur portable ou un PDA et à utiliser les outils fournis avec le pilote de son adaptateur WiFi pour mesurer la qualité du signal. On peut alors noter où se situent les éventuelles zones d'ombre et déplacer les AP jusqu'à trouver une configuration optimale.

Malheureusement, les outils d'analyse des adaptateurs sont souvent de qualité assez médiocre. Par exemple, le pilote Zero Config de Windows XP ne fournit que le débit physique négocié avec l'AP, sans indiquer le rapport signal/bruit ou le niveau précis du signal, comme le montre la figure 5.18. Dans cet exemple le débit théorique (c'est-à-dire le débit physique utilisé) est de 11 Mb/s.

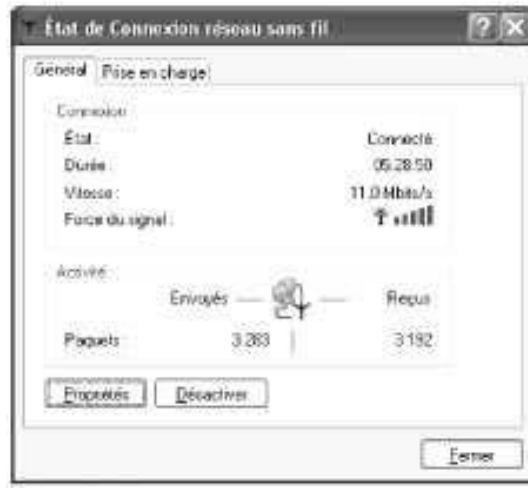


Figure 5.18 — Mesure rudimentaire du niveau de réception avec l'interface Zero Config.

1. Si la couverture radio est bonne, cela ne garantit pas forcément que la capacité sera bonne lorsque de nombreux utilisateurs téléchargeront en même temps. Pour cela, il faut faire des tests de charge.

Netstumbler

Une autre solution consiste à réaliser l'audit de site avec l'outil d'analyse Netstumbler, téléchargeable gratuitement sur *www.stumbler.net* (fig. 5.19). Il peut être installé sur un PC portable (sous Windows uniquement) ou un Pocket PC et il fournit de nombreuses informations sur la couverture radio, dont en particulier le niveau du signal, le RSB, le canal, le SSID et le BSSID de chaque AP à proximité. Malheureusement, il ne fonctionne pas avec tous les adaptateurs WiFi.

Il est également possible de le connecter à un module GPS (localisation par satellite) afin de générer automatiquement un plan du niveau de réception. Malheureusement, la réception GPS est en général impossible à l'intérieur d'un bâtiment, donc cette option n'est utile que pour les déploiements à l'extérieur. À l'intérieur, il est nécessaire de prendre note du niveau de réception pour chaque point du bâtiment.

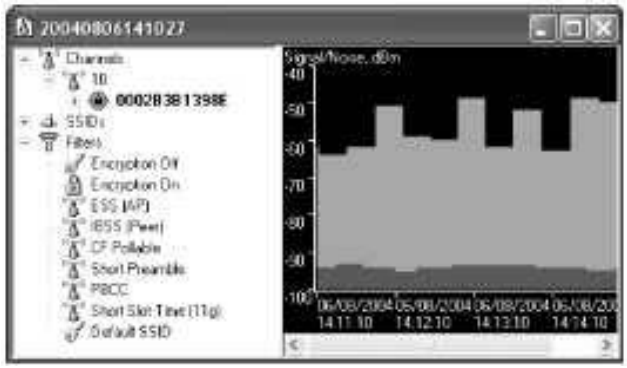


Figure 5.19 — Le logiciel Netstumbler en action.

Outils d' analyse professionnels

Les logiciels commerciaux spécialisés dans l'audit de site sont nombreux. Citons quelques-uns des plus répandus : AirDefense, AirMagnet (fig. 5.20), Finisar, Network Associates, WildPackets et YellowJacket. Certains sont disponibles à la fois pour PC portable et Pocket PC. En plus des paramètres indiqués par NetStumbler (niveau du signal, RSB, canal, SSID, BSSID), ces logiciels permettent d'obtenir de nombreuses autres informations importantes, dont en particulier le débit réel grâce à un mode « actif » dans lequel le logiciel s'associe au réseau sans fil et réalise des transferts de données avec lui-même, donc sans qu'il soit nécessaire de connecter l'AP au réseau filaire.

Par ailleurs, l'analyse des interférences et des pertes de paquets est souvent assez fine : certains produits sont même de véritables analyseurs de spectre de fréquences radio et peuvent détecter toutes les interférences avec précision (dans le produit YellowJacket, par exemple).

Certains sont couplés à une base de connaissance qui fournit un grand nombre de conseils pratiques pour la résolution de problèmes. Elle est particulièrement complète dans le produit AirMagnet.

Bref, ce type d'outils d'analyse est très utile pendant l'audit de site… mais aussi et surtout après l'installation du réseau sans fil, pour détecter d'éventuels problèmes apparus après l'installation : de nouvelles sources d'interférences, des tentatives d'intrusion dans le système ou encore des points d'accès pirates.

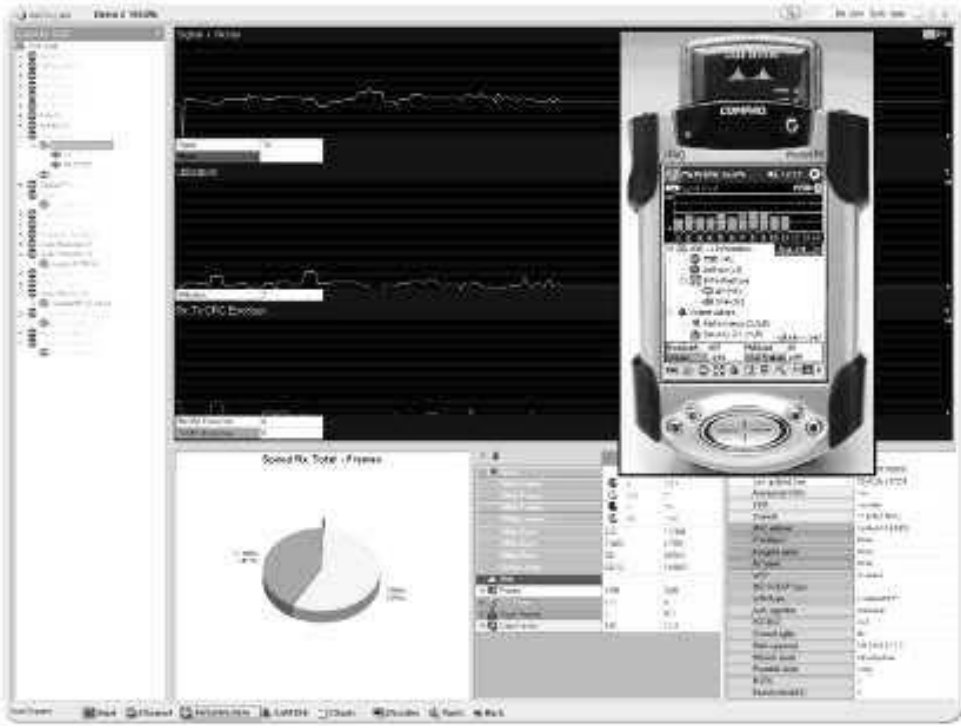


Figure 5.20 — Logiciels d'analyse AirMagnet, pour ordinateur portable ou PDA.

Outils de cartographie radio

Pendant un audit de site, certains outils d'analyse sont capables d'enregistrer les paramètres radio et de les associer à un point sur un plan des locaux. Ceci permet à la fois de visualiser la couverture radio, mais aussi de réaliser des simulations.

Par exemple, le logiciel Surveyor[1] de la société AirMagnet fonctionne de la façon suivante (fig. 5.21) :

- L'utilisateur commence par fournir au logiciel un plan des locaux, par exemple au format AutoCAD[2] ou bien plus simplement sous la forme d'une image, telle qu'une photographie numérique du plan d'évacuation des locaux – cette

1. « Audit de site » se dit *site survey* en anglais.
2. AutoCAD est un format de fichier très souvent utilisé en Conception assistée par ordinateur (CAO).

dernière option est souvent la façon la plus rapide d'obtenir un plan précis de n'importe quel bâtiment.

- On positionne sur ce plan les points d'accès que l'on a allumés.
- Ensuite, il suffit de se promener dans les locaux et de cliquer sur le plan en indiquant où l'on se situe, à intervalles réguliers : le logiciel fait une mesure à chaque clic et l'associe à la position de la souris sur le plan. Alternativement, on peut utiliser une fonction assez pratique de ce logiciel : on définit à l'avance un parcours sur le plan, puis il suffit de cliquer sur le bouton « départ », de suivre le parcours à vitesse constante puis de cliquer sur le bouton « arrivée » : le logiciel prend automatiquement les mesures pendant le parcours et détermine *a posteriori* où l'utilisateur se situait à chaque instant.

Avec cet outil, il est également possible d'effectuer quelques simulations : par exemple, que se passerait-il si la puissance d'émission de tel AP était plus faible, ou plus élevée ? Surveyor n'a toutefois pas vocation à être un logiciel de simulation complet : il est impossible de déplacer « virtuellement » un AP, de simuler l'ajout d'une antenne directionnelle ou encore l'impact d'un nouvel obstacle. Pour cela, il faut refaire une mesure sur le terrain. Le plan est un support visuel pour l'utilisateur mais il n'est absolument pas pris en compte par le logiciel pour ses calculs de propagation radio. Le but de ce produit n'est pas de modéliser, mais bien d'analyser.

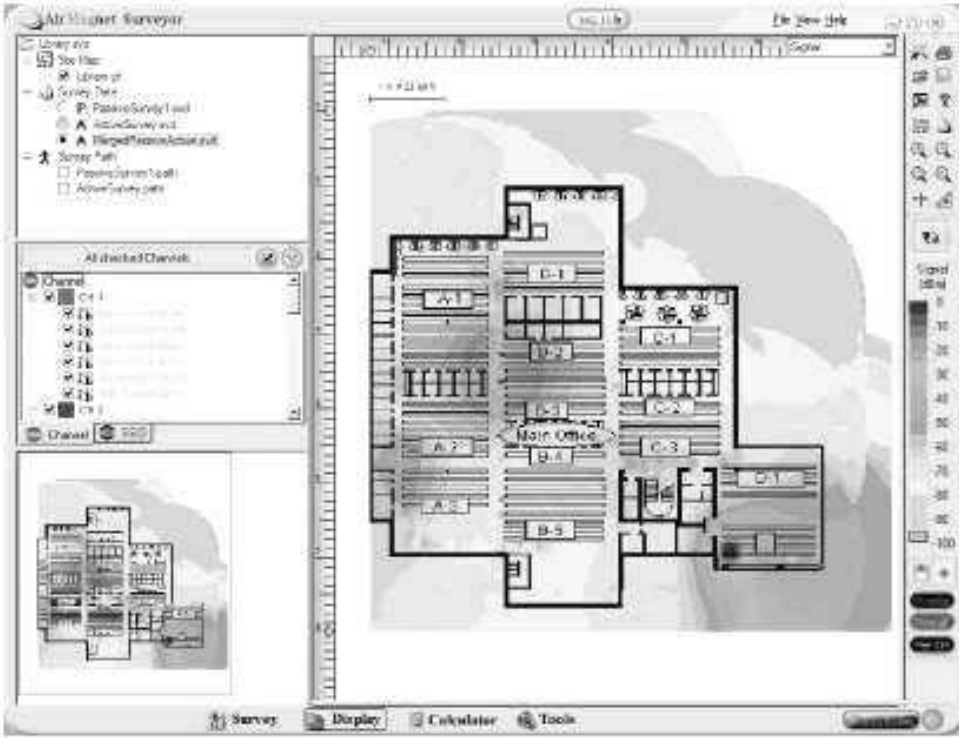


Figure 5.21 — Le logiciel de cartographie radio Surveyor.

On peut aussi visualiser la couverture radio de plusieurs façons différentes : d'abord en se focalisant uniquement sur le niveau de réception en chaque point pour visualiser les zones d'ombres, la quantité de débordement vers l'extérieur du bâtiment, ou encore les zones où la réception est insuffisante pour atteindre le débit minimal souhaité. Une autre vue permet de distinguer la zone de couverture de chaque AP, afin de mieux voir les zones de recouvrement et d'interférences entre AP utilisant le même canal.

Un autre avantage des logiciels de cartographie est la documentation : les cartes imprimées sont bien plus claires pour tout un chacun qu'une obscure liste de paramètres radio griffonnés sur une feuille de papier. Par ailleurs, il est intéressant de refaire régulièrement la cartographie radio après le déploiement pour observer d'éventuels changements de la couverture radio et de comparer la carte obtenue avec les précédentes : les changements sont plus alors bien plus faciles à remarquer.

Outils de simulation

À l'opposé de l'étude sur le terrain, ou plutôt en complément, il existe des outils de simulation de la couverture radio, comme le logiciel *Modeler* de la société OPNET (auquel il faut rajouter le module pour les réseaux sans fil) ou encore *RingMaster* de la société *Trapeze Networks* (fig. 5.22). À l'instar des outils de cartographie radio, il est nécessaire de fournir une carte au logiciel, mais ici une véritable analyse de la carte est réalisée et la participation de l'utilisateur est requise pour indiquer où se situent les obstacles et quelle est leur nature. Une fois la (longue) phase de paramétrage réalisée, le logiciel est capable de simuler diverses configurations d'AP et d'évaluer la couverture radio résultante.

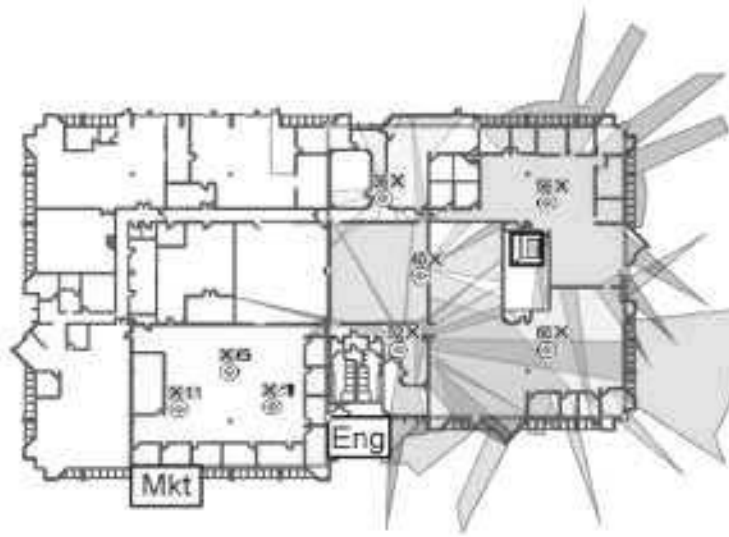


Figure 5.22 — Exemple de simulation radio du logiciel RingMaster.

Pour que le résultat d'une simulation soit significatif, il est nécessaire de saisir beaucoup d'informations, comme le plan des bureaux, la position des principaux

obstacles, le matériau et l'épaisseur des cloisons, etc. Il peut parfois s'agir de l'unique solution possible si un test sur le terrain est impossible : par exemple si le bâtiment est en construction !

Ces outils peuvent être utilisés avant l'audit de site pour avoir une idée du nombre d'AP nécessaires et de leur positionnement (au moins approximatif) pour obtenir la meilleure couverture et le meilleur débit, mais il est tout de même fortement conseillé de faire des analyses sur le terrain avant le déploiement proprement dit.

Le prix de ces logiciels est assez élevé, ce qui explique sans doute en grande partie pourquoi les audits de site sont encore de loin la solution préférée par les entreprises pour préparer les déploiements.

Les réseaux sans fil adaptatifs

Pour finir sur les outils d'aide au déploiement, on peut signaler que de plus en plus de professionnels du déploiement WiFi encouragent une approche radicalement différente du déploiement radio, en opposition au « traditionnel » audit de site : il s'agit des réseaux sans fil adaptatifs (fig. 5.23).

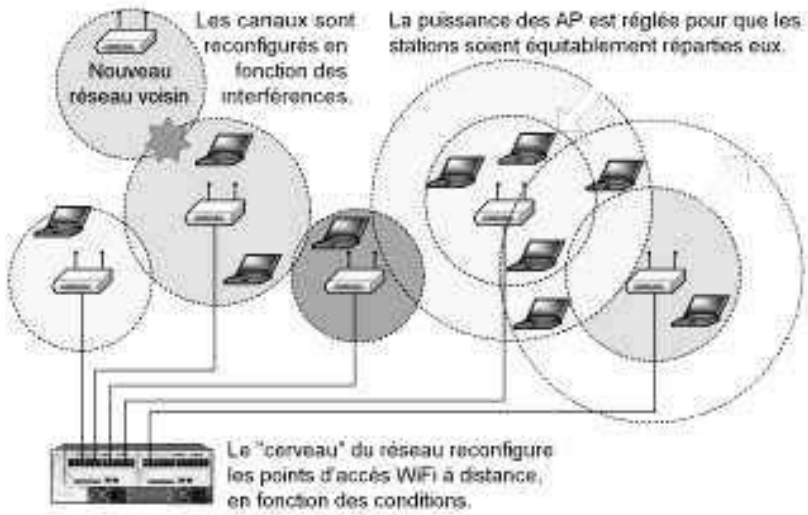


Figure 5.23 — Un réseau sans fil adaptatif.

Le principe est simple : on déploie une densité importante d'AP et on installe un logiciel capable de configurer automatiquement les AP pour éviter les interférences radio (entre autres avec les autres AP), afin d'atteindre la meilleure couverture possible. Cette configuration automatique peut être réalisée plusieurs fois par jour, sans intervention humaine et sans que les utilisateurs ne s'en aperçoivent. Les avantages des réseaux sans fil adaptatifs sont multiples :

- les audits de site ne sont plus nécessaires ;

- aucun nouveau déploiement ne sera nécessaire par la suite, même si la configuration des bureaux change ou bien que de nouvelles interférences font leur apparition ;
- le logiciel est capable de détecter qu'un AP est surchargé car trop d'utilisateurs y sont associés et dans ce cas il peut contrôler l'AP pour basculer quelques utilisateurs vers une cellule voisine. On peut donc optimiser non seulement la couverture du réseau sans fil mais également sa capacité, en permettant à de nombreux utilisateurs de se connecter en même temps.

Malheureusement, vous vous en doutez, cette solution est assez chère, d'une part parce que l'on doit installer plus d'AP qu'il ne serait réellement nécessaire (bien que le prix des AP soit nettement à la baisse le coût du câblage reste élevé) et d'autre part parce que le logiciel capable de tant de prouesses est loin d'être gratuit.

Parmi les solutions de ce type, citons celle de la société Aruba Wireless Networks. Dans le cas de la solution d'Aruba, les AP doivent être reliés à un commutateur « intelligent » dans lequel est installé le logiciel AirOS qui met en œuvre de nombreuses fonctions :

- le mécanisme de configuration automatique des AP ;
- le PoE (802.3af) pour alimenter les AP au travers des câbles réseau ;
- le STP pour éviter les boucles dans la topologie du réseau ;
- les VLAN (802.1q) pour avoir plusieurs réseaux virtuels sur la même infrastructure ;
- la QoS pour définir des classes de trafic et les gérer différemment ;
- la répartition dynamique des utilisateurs entre les AP ;
- la redondance complète : le commutateur possède par exemple deux alimentations électriques et deux séries de ports redondants qui sont utilisés en cas de panne (fig. 5.24) ;
- d'autres fonctions de sécurité avancées comme un pare-feu par utilisateur, le 802.1x, le WPA, etc. ;
- une interface web à partir de laquelle il est possible de gérer le réseau sans fil au complet et même de visualiser un plan du site et tous les AP déployés (pourvu bien sûr que cela ait été renseigné auparavant).

Bien qu'Aruba fabrique ses propres AP et que le système soit avant tout conçu pour fonctionner avec ceux-ci, le commutateur est capable de gérer certains AP d'autres constructeurs. Depuis 2005, de nombreux constructeurs se sont lancés sur le marché des commutateurs « intelligents » : les produits s'améliorent et les prix baissent. La société Meru Networks propose une solution similaire, mais avec une particularité originale: tous les point d'accès émettent sur un même canal, et se font passer pour un seul et même point d'accès virtuel. Du point de vue des stations qui se connectent au réseau, tout se passe exactement comme s'il n'y avait qu'un seul point d'accès. Cela peut paraître surprenant car on cherche plutôt, en général, à configurer sur des canaux différents les points d'accès situés à proximité les uns des autres. Mais puisque les points d'accès sont contrôlés par un commutateur « intelligent », ils sont bien synchronisés

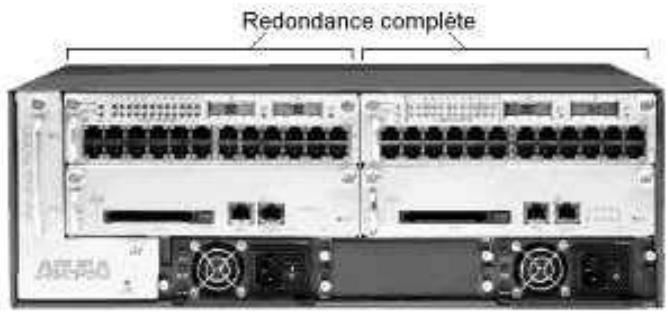


Figure 5.24 — Le commutateur « intelligent » d'Aruba, pour réseau sans fil adaptatif.

et n'émettent pas en même temps. En outre, puisqu'une station qui se déplace ne voit qu'un seul point d'accès, elle ne s'occupe pas du transfert (*hand-over*) d'un AP à un autre : tout est géré par le commutateur « intelligent », ce qui est appréciable car souvent les adaptateurs WiFi des stations gèrent mal le *hand-over*[1]. On se rapproche ainsi de l'architecture des réseaux GSM dans lesquels le réseau contrôle tout.

Pour finir, certaines solutions s'affranchissent du commutateur « intelligent », en répartissant la fonction de contrôle du réseau entre les différents points d'accès – ces AP sont appelés des « points d'accès à contrôle collectif » (*Collective Control Access Points*, ou CC-AP). Les CC-AP communiquent les uns avec les autres régulièrement, à l'aide d'un protocole propriétaire, pour mettre en œuvre les mêmes fonctions que celles mises en œuvre par les commutateurs « intelligents » : répartition de la charge entre les CC-AP, choix automatique des canaux radio, etc. Cette solution a plusieurs avantages sur les solutions reposant sur des commutateurs « intelligents » : elle est moins coûteuse, du moins pour les petits réseaux composés d'un nombre limité de CC-AP (car on s'affranchit du coût du commutateur « intelligent ») ; elle supporte mieux la montée en charge car le trafic n'est pas centralisé en un point ; et elle résiste mieux aux pannes, car si un CC-AP est défaillant, le reste du réseau continue à fonctionner normalement.

5.3.5 L'installation des AP

Pour clore ce chapitre, voici des conseils sur le déploiement proprement dit, c'est-à-dire l'installation et la configuration des AP. Le coût du déploiement est souvent dû en grande partie au câblage réseau nécessaire pour relier les AP entre eux et au réseau filaire. Une façon de réduire ce coût est de tirer profit de la technologie PoE (pour s'affranchir du câblage électrique) ou encore le CPL (pour s'affranchir du câblage réseau).

1. Très souvent, un adaptateur WiFi reste associé à un AP tant qu'il a un signal, même si ce signal est bien plus faible que celui d'un AP plus proche.

Le câblage réseau doit être de qualité professionnelle, éventuellement délégué à un prestataire. Il est très fréquent qu'un problème de débit soit dû à un câble défectueux ou un câblage mal réalisé, plutôt qu'aux ondes radio.

Il faut également s'assurer que les AP soient protégées contre les intempéries, l'humidité, la chaleur, les chocs, etc. Il existe des boîtiers conçus spécialement pour protéger les AP pour un déploiement à l'extérieur. La robustesse physique des AP et la qualité des connexions sont des critères importants de choix des AP : il ne faut pas que le câble d'antenne, la prise électrique, le câble réseau ou l'adaptateur WiFi puissent se détacher trop facilement.

Installer les AP à bonne distance (quelques mètres) des bureaux et les dissimuler, par exemple dans les faux-plafonds, permet de garantir la sécurité sanitaire des employés (voir le chapitre 11), mais aussi de limiter les risques de vols ou de dégradations, et enfin cela réduit la crainte des effets des ondes.

Enfin, si la topologie des bureaux le permet, il est bon de se garder la possibilité de déplacer les AP facilement et d'en installer de nouveaux, car la qualité de la réception peut changer si un voisin met en place un réseau sans fil ou bien si les bureaux changent de configuration. La question ne se pose évidemment pas dans le cas d'un réseau WiFi adaptatif.

Résumé

Dans ce chapitre, nous avons abordé le bilan radio, les règles de la propagation des ondes radio et les stratégies pour mettre en place un réseau sans fil offrant une bonne couverture et une haute capacité, notamment avec les commutateurs « intelligents ».

Faire le bilan d'une liaison radio consiste à s'assurer qu'il y ait une marge de puissance suffisante pour que la communication soit stable. Cette marge est égale à la puissance de l'émetteur (en dBm), plus le gain des antennes (en dBi), plus la perte dans les câbles et connecteurs d'antennes (en dB), plus la perte en espace libre (en dB) et moins la sensibilité du récepteur (en dBm). Pour qu'une liaison soit stable, on recommande que la marge, dans chaque sens, soit au moins égale à 6 dBm.

La puissance isotrope rayonnée équivalente (PIRE) d'un système est égale à la puissance de l'émetteur, plus le gain de l'antenne, plus la perte dans le câble d'antenne et les connecteurs. Il est limité par la législation selon la fréquence, les canaux utilisés, le lieu de déploiement et les fonctionnalités du matériel (voir le chapitre 11) pour un tableau récapitulatif de la réglementation française en matière de WiFi). Si l'émetteur est puissant, alors l'antenne doit avoir un faible gain afin de respecter la limite légale de PIRE. Dans ce cas, la portée est faible mais le faisceau rayonné est large. Inversement, si l'émetteur est faible, alors l'antenne peut être puissante : la portée est alors plus importante, mais le faisceau beaucoup plus étroit. Il faut trouver le bon équilibre en fonction du contexte.

TROISIÈME PARTIE

Sécurité

Cette troisième partie présente les solutions de sécurité que l'on peut mettre en place pour un réseau WiFi. Il s'agit de la partie la plus longue car c'est un sujet complexe et crucial :

- le chapitre 6 dresse un tableau général de la problématique de sécurité dans un réseau sans fil et présente les solutions simples permettant d'offrir un premier niveau de sécurité ;
- le chapitre 7 décrit le WEP, la solution de sécurité proposée par la première version du standard WiFi. Cette solution comporte malheureusement de nombreuses failles que nous présentons également ;
- le chapitre 8 détaille le protocole 802.1x et le protocole EAP sur lequel il repose. Ces protocoles ont pour rôle de permettre l'identification des utilisateurs et la mise en place d'une session sécurisée ;
- le chapitre 9 présente le WPA et le WPA2 (802.11i), qui reposent sur le 802.1x. Ce sont les meilleures solutions de sécurité du WiFi. Elles offrent un niveau de sécurité inégalé ;
- le chapitre 10 présente le protocole RADIUS et donne des indications sur l'installation et la configuration d'un serveur RADIUS, essentiel dans l'architecture WPA Enterprise ;
- le chapitre 11 présente les réglementations à respecter lorsque l'on déploie un réseau WiFi, en détaillant les questions de santé.

6

La sécurité sans fil

Objectif

La question de la sécurité est sans doute la première que se pose une société lorsqu'elle se penche sur le WiFi. Si l'on communique à travers les ondes, tout le monde peut capter les communications, n'est-ce pas ? Face à cette crainte, de nombreux dirigeants d'entreprises ont eu un réflexe de prudence : attendre quelques mois ou quelques années pour bénéficier du retour d'expérience d'autres entreprises. Ils ont peut-être eu raison d'ailleurs, car les débuts de la sécurité en WiFi n'ont pas été glorieux. Heureusement, il existe à présent des solutions très robustes pour rendre un réseau sans fil tout aussi sécurisé qu'un réseau filaire. Toutefois, ces solutions sont loin d'être triviales, et c'est pourquoi nous avons consacré tant de chapitres à la sécurité. Dans ce chapitre, nous commencerons par définir ce qu'est la sécurité dans un environnement sans fil, et nous ferons le tour des solutions de sécurité existantes. Nous détaillerons les plus importantes d'entre elles au cours des chapitres suivants.

6.1 INTRODUCTION À LA SÉCURITÉ

6.1.1 Définir la sécurité

Réduire les risques

La première fonction d'un système d'information est de stocker et de permettre l'échange de données. Sécuriser un système d'information consiste donc à réduire le risque que les données soient compromises ou qu'elles ne puissent plus être échangées. En outre, si un système informatique contrôle, par exemple, des équipements industriels ou le trafic aérien, alors on peut imaginer toutes sortes de catastrophes bien pires que quelques données compromises !

Sécuriser un réseau consiste donc à prendre en compte tous les risques possibles, tels que les attaques volontaires, les accidents, les défauts logiciels ou matériels, ou encore les erreurs humaines et à les réduire autant que possible.

Les qualités CID

Trois qualités fondamentales sont à attendre d'un réseau sécurisé. On les appelle les qualités CID (d'après leurs initiales) :

- **La confidentialité** : l'accès aux données (et d'une façon générale aux ressources gérées par le système) doit être réservé aux personnes autorisées. Cela suppose un mécanisme d'identification des utilisateurs, la définition de règles d'accès, et la protection des données pendant leur transport, par le biais d'un cryptage[1].
- **L'intégrité** : les données ne doivent pas être modifiées ou perdues. Il faut en particulier pouvoir s'assurer que ce qui est reçu correspond bien à ce qui a été envoyé.
- **La disponibilité** : le réseau doit être accessible en tout temps et dans des conditions acceptables.

La non-répudiation

Les experts en sécurité informatique définissent souvent une quatrième qualité que doit posséder un système sécurisé : la « non-répudiation ». Il s'agit de la possibilité de prouver *a posteriori* qu'une personne a bien participé à une transaction donnée. Par exemple, si un client s'est connecté au système d'information et a passé une commande, il ne faut pas qu'il puisse prétendre plus tard ne jamais l'avoir fait.

La notion de non-répudiation est donc très liée à la législation en vigueur : un juge acceptera-t-il une simple ligne dans une base de données comme preuve que le client a bien passé la commande et qu'il doit la payer ? Qui peut prouver que cette fameuse ligne n'a pas été rajoutée suite à une erreur du système ou par une personne mal intentionnée ?

Une solution consiste à mettre en place une architecture permettant aux transactions importantes d'être signées électroniquement par leur(s) auteur(s). Dans notre exemple, il sera plus difficile au client de prétendre qu'il n'a jamais passé de commande si la société peut montrer que celle-ci a été signée électroniquement.

Les nouvelles solutions de sécurité du WiFi sont très robustes et permettent de garantir les qualités CID, grâce à une authentification sûre, un cryptage puissant et divers autres mécanismes sophistiqués. En outre, le protocole 802.1x, que nous étudierons au chapitre 8 et qui sert à identifier les utilisateurs WiFi à la connexion, est suffisamment souple pour identifier les utilisateurs selon de multiples méthodes : mot de passe, carte à puce, etc. Certaines de ces méthodes exigent de l'utilisateur qu'il prouve qu'il possède bien un certificat électronique. En utilisant cette méthode d'authentification et en enregistrant les échanges entre le poste de l'utilisateur et le

1. Nous utilisons le mot « cryptage », d'autres parlent de « chiffrement » : ce sont des synonymes.

serveur au moment de l'authentification, il sera possible de prouver *a posteriori* que cet utilisateur avait bien utilisé son certificat pour se connecter. Malheureusement, ce qui se passe par la suite au cours de la session de l'utilisateur sur le réseau n'est pas signé et donc on ne peut pas prouver que l'utilisateur en est l'auteur. On peut donc dire que la non-répudiation n'est pas réellement au programme du WiFi : si elle doit être mise en œuvre, il faudra qu'elle le soit au niveau des couches réseaux supérieures.

Un réseau sécurisé assure la confidentialité, l'intégrité et la disponibilité des données et si possible la non-répudiation des transactions.

6.1.2 Une politique globale

L'ingénierie sociale

Les employés de votre société laissent-ils traîner des documents confidentiels sur leur bureau ? Oublient-ils leurs impressions dans l'imprimante et leurs fax dans la télécopieuse ? Leurs mots de passe ressemblent-ils à « lucie » ou « vincent73 » ? Si leurs mots de passe ressemblent plutôt à « f9jKx$D2 », les collent-ils sur leurs écrans avec des étiquettes pour ne pas avoir à les retenir ? Si, si, c'est très fréquent !

Parce que la sécurité est souvent prise à la légère par les employés, une discipline de sécurité très particulière connaît un grand succès : « l'ingénierie sociale ». Elle consiste à évaluer le niveau de sécurité d'un système par une méthode simple : tenter d'extraire le maximum d'informations compromettantes en profitant de la naïveté ou de la désinvolture des employés.

L'expert en ingénierie sociale est mandaté par une société pour en auditer la « sécurité sociale ». Il peut commencer par vérifier s'il peut pénétrer dans les locaux de l'entreprise simplement en se présentant à l'accueil comme un client pressé, par exemple[1]. Une fois rentré, il peut chercher tous les documents qui traînent. Il peut discuter avec des employés, en se faisant passer par exemple pour un nouvel employé et essayer d'obtenir tout type d'information. S'il trouve un bureau inoccupé, il peut s'y installer et avec un peu de chance, il trouvera peut-être un mot de passe inscrit sur le coin d'une feuille de papier. Sinon, il peut téléphoner au support informatique, se faire passer pour un employé, et prétendre avoir oublié son mot de passe. S'il parvient à obtenir un mot de passe d'accès au réseau et à s'y connecter, on peut dire qu'il aura gagné la partie et pourra aller rédiger un rapport croustillant. Heureusement, son rôle est de dresser un état des lieux : il se contente donc d'espionner, mais ne va pas jusqu'à détruire des données. Cependant, un pirate serait bien moins scrupuleux.

Le maillon faible

Le but du paragraphe précédent était de vous montrer à quel point la sécurité mise en place au niveau WiFi peut devenir dérisoire si elle n'est pas accompagnée d'une politique de sécurité globale. Pour assurer la sécurité des données d'un système, il ne

1. Pour être plus rigoureux, il faudrait distinguer ici l'évaluation de la sécurité physique et celle de la sécurité sociale, mais les deux sont souvent liées.

suffit pas d'installer tel ou tel matériel ou de choisir telle ou telle technologie. En effet, le niveau de sécurité d'un système est égal au niveau de sécurité de son maillon le plus faible.

> La sécurité en entreprise doit faire l'objet d'une politique globale : les technologies et les protocoles n'en sont qu'une petite partie.

Tout l'enjeu d'une politique de sécurité consiste donc à regarder le système dans son ensemble, à identifier les vulnérabilités les plus graves et les plus probables, et à y remédier. Idéalement, l'ensemble des processus doit être analysé en prenant en compte les aspects humains, techniques, légaux, organisationnels et stratégiques. Pour cela, il est recommandé qu'une personne supervise la sécurité à l'échelle de la société et donne des directives appliquées à tous les échelons. Cela peut passer par la sensibilisation des employés, la formation des équipes techniques et des contrôles réguliers.

6.1.3 La compartimentation

Les pirates de l'intérieur

Il peut arriver qu'une personne extérieure à l'entreprise, telle qu'un client, un fournisseur ou tout autre visiteur, ait accès au réseau pendant quelques heures voire quelques jours. Si la simple connexion au réseau donne accès à des données confidentielles, alors ces visiteurs seront peut-être tentés de les consulter, les copier, ou pourquoi pas, les modifier. Le visiteur devient pirate ! Plus simplement, il peut s'agir d'un employé peu scrupuleux, qui souhaite voir combien gagnent ses collègues ou lire leurs courriers électroniques. Bref, il faut malheureusement se méfier de tout et de tout le monde. Comme le dit Andrew S. Grove, cofondateur d'Intel : « *Only the paranoid survive* »[1].

Si les attaques peuvent venir de l'intérieur, la seule solution pour garantir un niveau de sécurité acceptable consiste à compartimenter les données. En d'autres termes, les données qui concernent uniquement un employé ou un groupe d'employés ne doivent être visibles que par cet employé ou ce groupe. Par exemple, seuls les commerciaux auront accès à la base des clients, seules les ressources humaines auront accès aux *curriculum vitae* des postulants, etc. Un bémol toutefois, ce type d'organisation compartimentée n'est pas particulièrement à la mode aujourd'hui : l'heure est plutôt à l'ouverture et à la décompartimentation. Il faut donc savoir trouver le bon niveau de compartimentation qui permette d'assurer le maximum de sécurité sans bloquer l'activité quotidienne.

Méthodes de compartimentation

Pour isoler les utilisateurs et éviter qu'ils aient accès à tout le trafic réseau, une mesure simple mais importante consiste à installer des commutateurs (*switchs*) plutôt que de simples répétiteurs (*hubs*). Ceci permet à la fois d'augmenter la capacité du réseau filaire et de le sécuriser davantage, car le commutateur ne relaie chaque paquet que

1. « Seuls les paranoïaques survivent ».

vers son destinataire, contrairement au répétiteur qui, comme son nom l'indique, se contente de répéter le paquet à tout le monde.

Une solution plus sûre consiste à utiliser des commutateurs et des points d'accès (AP) capables de gérer des LAN virtuels (VLAN) selon la norme IEEE 802.1Q (voir le chapitre 4, § 4.2.3). Par exemple, un VLAN pourrait être limité à la comptabilité, un autre aux commerciaux, un autre à la direction, et un dernier serait accessible à tous... le tout sur la même infrastructure réseau !

Installer un pare-feu sur chaque poste et chaque serveur permet de diminuer le risque de piratage : même si un pirate a accès au réseau, il aura du mal à accéder à un service bloqué par un pare-feu sur un autre poste.

Par ailleurs, si un ordinateur portable se fait voler, il est préférable que les données qui s'y trouvent ne puissent pas être lues par le voleur. Le plus simple consiste à utiliser des disques durs cryptés.

> Si les employés sont amenés à se déplacer fréquemment avec leur ordinateur portable professionnel, il est fortement recommandé d'utiliser des disques dur cryptés. Un mot de passe est alors demandé à l'utilisateur à l'allumage de l'ordinateur : sans lui le disque dur est illisible.

On peut aller encore plus loin en déployant sur tout le réseau un système de contrôle qui permette de limiter l'accès aux services à des utilisateurs identifiés et autorisés : on peut utiliser, par exemple, la solution Kerberos développée par le *Massachusetts Institute of Technology* (MIT), ou encore une Infrastructure à gestion de clés (IGC), également appelée *Public Key Infrastructure* (PKI).

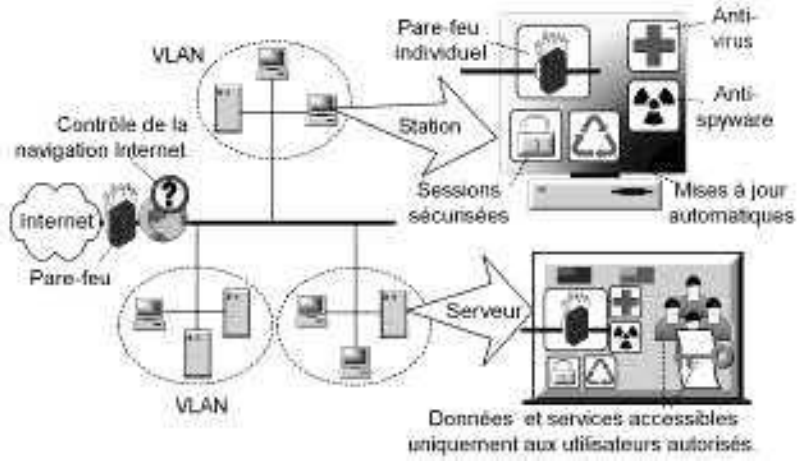


Figure 6.1 — Un réseau compartimenté.

Accéder au contrôle total d'un réseau est le Saint-Graal du pirate, et cela suppose en général de se faire passer pour un utilisateur légitime. Toutefois, si le réseau est bien compartimenté, le fait d'être connecté au réseau n'implique pas que toutes les

données soient accessibles. Si un pirate parvient à usurper l'identité d'un utilisateur qui n'a que peu de droits sur le réseau, il n'est pas très avancé !

La sécurité d'un système peut être vue comme une ville médiévale, entourée de plusieurs cercles concentriques de murailles : l'envahisseur doit franchir toutes les murailles pour prendre le contrôle de la cité.

6.1.4 La connexion à Internet

Installer un pare-feu pour protéger la connexion à Internet est un strict minimum. Mais ce n'est souvent pas suffisant. La loi française, renforcée par la jurisprudence, stipule que si un employé utilise la connexion à Internet de son entreprise pour faire quelque chose d'illégal – par exemple l'envoi de milliers d'e-mails (ou *spam*), la fraude à la carte bleue, la diffamation ou encore l'incitation à la violence ou à la haine raciale – alors la responsabilité de l'entreprise est engagée ! Il ne suffit donc pas d'être capable d'identifier le fautif : il faut l'arrêter avant qu'il ne nuise ou en tout cas être en mesure de montrer qu'on a fait le maximum pour empêcher que cela n'arrive. On a donc l'obligation légale de contrôler l'accès à Internet !

> Le propriétaire d'une connexion à Internet en est responsable : si cette connexion est utilisée à des fins illégales, sa responsabilité peut être engagée.

Mais il y a également bien d'autres raisons de limiter l'accès à Internet : le risque d'infection par des virus informatiques ou par du *spyware*[1], le risque de diffusion de données confidentielles, le risque de dégradation de l'image de l'entreprise, et simplement le risque de perte de productivité des employés ! Il existe sur le marché de nombreux logiciels de contrôle de la navigation Internet (on parle de « contrôle de contenu »), dont par exemple *Websense* ou *SurfControl*.

Toutefois, il faut faire attention, car il existe également des lois protégeant l'employé[2] : par exemple, un courrier électronique dont le titre précise que le contenu est privé ne doit pas être lu. La société se trouve donc coincée entre l'obligation de contrôler l'usage de sa connexion à Internet et l'obligation de respecter la vie privée de ses employés.

6.1.5 L'évolution de la sécurité

Pour clore cette brève introduction à la sécurité informatique, notons qu'un système parfaitement sécurisé aujourd'hui ne sera sans doute plus tout à fait sécurisé dans

1. Un *spyware* est un logiciel espion qui envoie des informations concernant l'utilisateur à une personne ou une société qui pourra en tirer parti. Souvent, il surveille la navigation web de l'utilisateur dans le but de discerner ses habitudes et de pouvoir lui envoyer des offres commerciales susceptibles de le séduire.
2. Voir le site de la Commission nationale de l'informatique et des libertés (CNIL) pour en savoir plus : *www.cnil.fr*.

un an, si l'on ne le met pas à jour. De nouvelles failles auront été découvertes, à tous les niveaux et surtout au niveau logiciel. L'exemple le plus simple est le virus informatique : si vous avez un antivirus installé sur votre ordinateur (si ce n'est pas le cas, courrez vite en installer un), vous savez qu'il faut le mettre à jour plusieurs fois par mois, voire automatiquement tous les jours. C'est le cas également des systèmes d'exploitation qui ont régulièrement des mises à jour de sécurité.

Il en va de même avec le WiFi : la solution de sécurité WPA2/AES (cf. § 6.4.4) semble très robuste, mais on ne peut pas af?rmer avec certitude qu'elle ne comporte aucune faille. Il faut rester sur le qui-vive. D'ailleurs, une faille a récemment été découverte dans le WPA/TKIP (cf. § 6.4.3).

6.2 LES ATTAQUES D'UN RÉSEAU WIFI

Après cette brève introduction à la sécurité informatique, passons maintenant au WiFi. Pour commencer, nous allons voir comment un réseau WiFi peut être attaqué.

6.2.1 Le wardriving

À la recherche des réseaux WiFi

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

- le signal ne porte pas très loin, donc le risque qu'un pirate trouve le réseau est faible ;
- il y a peu de pirates et beaucoup de réseaux WiFi, donc pourquoi un pirate s'attaquerait-il au mien plutôt qu'à un autre ?
- je ne suis qu'un simple particulier (ou une petite société), donc un pirate n'aurait aucun intérêt à me causer du tort ;
- je n'ai pas de données confidentielles, donc je ne risque rien.

Toutes ces excuses sont à proscrire ! Voici pourquoi : dès lors que l'on su que de nombreux réseaux WiFi n'étaient pas sécurisés, un nouveau « sport » est né : le *wardriving*[1] . Le plus souvent pratiqué par des groupes de passionnés de la radio, il consiste à se promener en voiture avec une antenne WiFi et à noter la position et les caractéristiques de tous les AP que l'on puisse trouver. Des logiciels tels que NetStumbler permettent même d'automatiser la tâche, et peuvent être reliés à un module GPS[2] pour que la position exacte soit enregistrée. La carte des points d'accès ainsi obtenue est souvent publiée sur Internet, de sorte que n'importe qui peut savoir où se situent les réseaux non sécurisés ! Ce phénomène est très loin d'être anecdotique : la popularité du *wardriving* est telle que des cartes sont disponibles pour des pays entiers.

1. Que l'on peut traduire par « la guerre en voiture ».
2. *Global Positioning System* : système de localisation par satellite.

Il existe même des concours entre plusieurs équipes, la gagnante étant celle qui détecte le maximum de réseaux en un temps limité. Il est tout de même important de noter que le *wardriving* est interdit par la loi, en France, comme bien sûr le fait de violer un système informatique, cela va sans dire !

Il existe un débat enflammé dans le monde de la sécurité pour savoir s'il faut, ou non, rendre publiques les vulnérabilités d'une technologie lorsqu'elles sont découvertes, avant de disposer d'une parade. En effet, les rendre publiques, c'est donner des outils aux pirates, mais c'est aussi informer les victimes potentielles et encourager la recherche de solutions. Certains adeptes du *wardriving* estiment que cette activité participe au renforcement de la sécurité du WiFi. À vous de juger.

Figure 6.2 — Exemple de carte de *wardriving,* publiée sur Internet.

Conséquences du wardriving

Quoi qu'il en soit, la première conséquence du *wardriving* est que vous ne devez en aucun cas supposer que votre réseau est invisible : quelques semaines seulement après son installation, il est bien possible qu'il soit référencé sur un site web !

Deuxième conséquence : le nombre de pirates potentiels est accru : en plus des pirates réellement mal intentionnés (rares mais très nuisibles), on doit maintenant prendre en compte les simples curieux, qui peuvent également nuire, ne serait-ce qu'en consommant votre bande passante. En outre, de plus en plus de personnes sont en train de comprendre l'importance de sécuriser leur réseau sans fil, donc si vous ne sécurisez pas le vôtre, les pirates se tourneront de plus en plus vers vous.

Par ailleurs, croire qu'un pirate a besoin d'une raison valable pour vous nuire serait bien naïf : de nombreux pirates veulent simplement voir jusqu'où ils peuvent aller, par jeu, par orgueil ou simplement pour acquérir une nouvelle compétence. Sous le couvert de l'anonymat que peut procurer une connexion WiFi peu sécurisée, certains vandalisent autant que possible un système, pour raconter ensuite leurs prouesses à des amis. Donc si vous pensez qu'un pirate n'aurait rien à gagner à vous nuire, détrompez-vous.

Pour finir, même si vous croyez n'avoir aucune donnée confidentielle, un pirate peut tout de même vous nuire : tout d'abord, il y a presque toujours des données confidentielles à protéger, quoi qu'on pense. Pensez au courrier électronique, aux

mots de passe d'accès à votre machine, aux sites sur lesquels vous naviguez. Même si vous n'avez réellement rien à cacher, le pirate peut vous nuire en effaçant des fichiers, en modifiant des données, en vous empêchant d'accéder à Internet ou à vos machines. Enfin, même s'il ne fait que naviguer sur Internet, n'oubliez pas qu'en tant que propriétaire de la connexion, vous en êtes responsable : si le pirate en abuse, par exemple en téléchargeant des fichiers interdits, vous pouvez en être tenu responsable !

Bref, la sécurité n'est pas une paranoïa d'experts cherchant à valoriser leur spécialité : c'est une réalité. Définissons maintenant rapidement les catégories d'attaques contre lesquelles nous devons nous prémunir : l'espionnage, l'intrusion, la modification des messages, le déni de service et la relecture.

6.2.2 L'espionnage

Sans doute la première attaque qui vient à l'esprit lorsque l'on parle des technologies sans fil est l'écoute : un pirate se poste à proximité et surveille les échanges. On dit qu'il « sniffe » le réseau sans fil. Dans les réseaux filaires, ceci est rendu difficile par le fait qu'il faut d'abord se brancher physiquement au réseau avec un câble avant de pouvoir écouter quoi que ce soit[1]. Avec le WiFi, chacun peut écouter ce qui est transmis par les autres. Il suffit pour cela de disposer d'un adaptateur WiFi gérant le mode *monitor*, c'est-à-dire capable de lire tous les messages, et pas uniquement ceux qui lui sont adressés[2]. Ensuite, il faut utiliser un logiciel d'analyse du réseau, du type Ethereal, pour « sniffer » tout ce qui se passe sur le réseau ! Écouter une communication WiFi est à la portée de presque tout le monde.

L'espionnage peut aboutir à la divulgation d'informations confidentielles : mots de passe, documents secrets, numéros de cartes bancaires, etc. Aussi, pour sécuriser les échanges, il est indispensable de crypter les communications avec un algorithme aussi puissant que possible, sans que cet algorithme ne ralentisse trop la communication. Nous verrons que le WPA et le WPA2 réalisent des cryptages très efficaces.

6.2.3 L'intrusion

Intérêt de l'intrusion

Une autre attaque consiste à s'introduire au sein du réseau WiFi pour consulter voire modifier les données du système informatique (bases de données, fichiers, e-mails...) ou encore pour profiter de la connexion à Internet.

1. Ceci n'est pas tout à fait exact : lorsqu'un signal électrique passe dans un câble, il génère une légère perturbation du champ électromagnétique, de sorte qu'avec un équipement adapté, il est possible de détecter à distance l'information qui y transite ! L'équipement nécessaire n'est toutefois pas à la portée du premier venu et il faut se situer à quelques mètres au maximum du câble.
2. En mode « *monitor* » on peut « sniffer » tous les paquets WiFi qui sont émis sur un canal choisi. Le mode « *promiscuous* » est semblable mais il suppose que l'on s'associe au préalable à un réseau sans fil, et l'on ne peut écouter que les paquets émis sur ce réseau.

Une intrusion réussie permet au pirate de se comporter exactement comme un utilisateur normal : au point qu'il est souvent difficile de s'apercevoir qu'une intrusion a eu lieu ou même qu'elle est en cours, car tout se passe comme si un utilisateur normal accédait au système. Il s'agit donc d'une attaque extrêmement dangereuse.

L'intrusion est bien sûr tout à fait triviale si aucune sécurité n'est mise en œuvre : il suffit de s'associer normalement à l'un des AP du réseau, et le tour est joué. En revanche, si l'association impose un mécanisme d'identification avant d'autoriser l'ouverture d'une session sur le réseau, le pirate aura essentiellement deux options :

- ouvrir une nouvelle session en se faisant passer pour un utilisateur légitime ;
- détourner une session existante (*hijacking*).

Attaque de dictionnaire

Pour la première option, le pirate doit parvenir à tromper le mécanisme d'identification. Par exemple, si les utilisateurs sont identifiés avec un mot de passe, il s'agit de trouver un mot de passe valable. Pour cela, le pirate a plusieurs options : si les mots de passe sont échangés « en clair » (c'est-à-dire qu'ils ne sont pas cryptés), il suffit d'attendre qu'un utilisateur légitime se connecte et d'espionner l'envoi de son mot de passe. Si le mot de passe est crypté, on peut essayer de s'attaquer à l'algorithme de cryptage utilisé, certains étant beaucoup plus faibles que d'autres.

Une autre technique, plus brutale, consiste à essayer des millions de mots de passe jusqu'à trouver le bon ! Certains logiciels permettent d'essayer les mots de passe les plus probables en utilisant les mots du dictionnaire, et en les modifiant légèrement. On parle donc d'attaques de « dictionnaire ». Des mots de passe constitués de prénoms et de chiffres sont particulièrement vulnérables à ce type d'attaques, de même que des mots de passe du type « admin », « test », « toto » ou « pass ». Les attaques de dictionnaire sont redoutables si les employés ne sont pas tous informés du risque des mots de passe trop simples.

Il existe deux variantes de l'attaque de dictionnaire : l'attaque « en ligne » et l'attaque « hors-ligne ». La première est la plus simple : l'utilisateur cherche à se connecter au système et il essaie successivement chaque mot de passe jusqu'à trouver le bon. Cette attaque a plusieurs inconvénients (pour le pirate) : d'une part, elle prend beaucoup de temps car chaque mot de passe doit être vérifié par le système, et d'autre part, le pirate risque d'être repéré, surtout si le système est configuré pour détecter les tentatives d'intrusion. En outre, le système peut mettre en œuvre des « contre-mesures », en bloquant toute nouvelle tentative après trois échecs, par exemple. Une bonne façon de se prémunir contre les attaques de dictionnaire en ligne est donc de configurer le système pour qu'il prévienne un administrateur lorsqu'un utilisateur essaie de nombreux mots de passe d'affilée, et que cet utilisateur soit automatiquement bloqué.

L'attaque « hors-ligne » est beaucoup plus sournoise. De nombreux protocoles d'authentification fonctionnent de la façon suivante : le serveur envoie un « défi » au client, c'est-à-dire un texte aléatoire, et ce client doit utiliser ce défi ainsi que son mot de passe pour générer sa réponse, selon un algorithme précis. Le serveur utilise alors le

même algorithme pour vérifier que la réponse est la bonne, donc que le mot de passe est le bon. L'attaque de dictionnaire hors-ligne fonctionne ainsi : le pirate enregistre le dialogue d'une authentification réussie. Il possède alors le défi et la réponse, correcte, de l'utilisateur. Rien ne l'empêche alors, hors connexion, d'essayer des millions de mots de passe (avec le même défi et le même algorithme), jusqu'à trouver celui qui donne la même réponse que celle donnée par l'utilisateur. Non seulement cela ira beaucoup plus vite que l'attaque en ligne, mais en plus le pirate n'aura aucune chance de se faire détecter ou bloquer. Seules deux parades sont possibles : utiliser une méthode d'authentification invulnérable aux attaques hors-ligne (nous les étudierons au chapitre 8), ou obliger tous les utilisateurs à utiliser un mot de passe extrêmement long et complexe. Cette deuxième option est rarement réalisable et c'est pourquoi les méthodes d'authentification vulnérables aux attaques hors-ligne doivent être évitées.

Idéalement, les mots de passe des utilisateurs doivent être assez long et complexes pour qu'il soit impossible de les deviner en quelques tentatives, le système doit détecter et bloquer les attaques de dictionnaire en ligne, et il doit également utiliser un protocole d'authentification invulnérable aux attaques de dictionnaire hors-ligne.

Attaque de relecture

Une autre façon d'ouvrir une nouvelle session consiste à enregistrer les paquets émis par une station légitime au moment où elle se connecte, puis de les émettre à l'identique un peu plus tard. Les relectures peuvent également servir à répéter tout type de requête, par exemple une insertion dans une base de données, avec toutes les conséquences que cela peut avoir. Une façon d'éviter les risques de relectures consiste à imposer qu'un compteur soit incrémenté à chaque paquet échangé : on dit qu'on rajoute du « sel » (*salt*) dans chaque paquet. De cette façon, un paquet contenant un compteur ancien sera rejeté. Le WEP n'offre aucune protection contre la relecture, mais en revanche le WPA2/AES (cf. § 6.4.4) est immunisé contre ce genre d'attaque, comme nous le verrons au chapitre 9.

Détourner une session existante

Le détournement de session est un peu plus compliqué à concevoir. Prenons un exemple pour illustrer ce dont il s'agit : Michel veut aller à une fête à laquelle il n'est malheureusement pas invité. Un gardien contrôle l'entrée, en demandant à chacun sa carte d'identité et en vérifiant qu'il figure bien dans la liste des invités. Difficile de tromper ce gardien sur la base de la carte d'identité.

Toutefois, afin de permettre aux invités de rentrer et de sortir sans avoir à présenter leur carte d'identité à chaque fois, le gardien fournit à chaque invité un bracelet nominatif. C'est là que se trouve la faille de sécurité : Michel attend qu'un invité soit admis et reçoive son bracelet. Il espionne la scène et parvient à voir le nom de l'invité : mettons « Marc ». Michel fabrique alors un bracelet parfaitement identique à celui de Marc et le présente au gardien. Celui-ci n'y voit que du feu, et Michel peut allègrement aller faire la fête.

Le principal risque pour Michel est que quelqu'un se rende compte que deux invités portent le même nom. S'il est particulièrement prudent, il peut choisir d'attendre que Marc s'absente pendant quelques minutes avant d'aller à la soirée.

Cette stratégie a un autre inconvénient du point de vue du pirate : si Marc prévient le gardien quand il s'en va pour de bon, celui-ci arrêtera Michel la prochaine fois qu'il cherchera à passer.

Et en WiFi...

Comment cet exemple s'applique-t-il au WiFi ? L'identification des utilisateurs est souvent un mécanisme assez coûteux en temps et en ressources informatiques : elle suppose en général l'accès à une base de données des utilisateurs. Il serait inconcevable de mettre en œuvre le mécanisme complet d'identification à chaque fois qu'un paquet de données est reçu, de la même manière que le gardien ne peut pas vérifier les cartes d'identité à chaque fois qu'un invité entre ou sort ! Du coup, l'identification initiale aboutit à la mise en place d'une identification « secondaire » valable pour la durée de la session.

Une solution courante consiste à utiliser simplement l'adresse réseau (c'est-à-dire l'adresse MAC, voir le chapitre 3, § 3.1.2) du poste de l'utilisateur qui a été identifié. Par exemple, si on a bien identifié l'utilisateur « Marc » à l'adresse « 00:0E:A6:5C:80:37 », on accepte dorénavant tous les paquets de données en provenance de cette adresse : c'est l'équivalent du bracelet dans notre histoire.

Malheureusement, il existe des adaptateurs WiFi dont on peut changer l'adresse MAC. Ceci permet à un pirate de facilement détourner des sessions : il lui suffit d'espionner le réseau en attendant l'arrivée d'un utilisateur légitime. Une fois que celui-ci s'est identifié, le pirate regarde quelle est l'adresse MAC de cet utilisateur et configure son propre adaptateur WiFi pour imiter cette adresse : on parle de *spoofing* de l'adresse MAC (fig. 6.3).

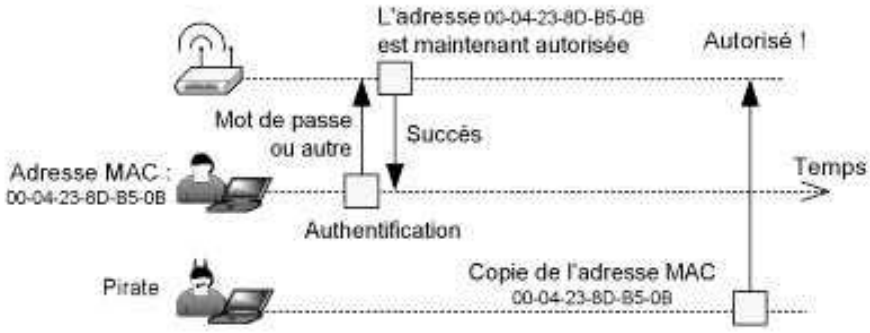


Figure 6.3 — Détournement de session par « *spoofing* » de l'adresse MAC.

L'identification secondaire (à chaque paquet) est donc tout aussi importante que l'identification primaire (à l'ouverture de la session sur le réseau). Nous verrons que

les solutions les plus robustes, mises en œuvre par le WPA et le WPA2, consistent à négocier, lors de l'identification primaire, l'échange sécurisé de clés de cryptage. De cette façon, un pirate ne peut pas détourner une session en cours, car il ne connaît pas les clés de cryptage à utiliser.

Si l'on a un système qui assure une bonne identification primaire, l'échange de nouvelles clés de cryptage au cours de cette identification, le puissant cryptage des communications avec ces clés pendant toute la durée de la session (ce qui garantit qu'une session ne peut pas être détournée facilement), et enfin une bonne résistance aux attaques de relecture, alors on peut dire que l'on possède un bon niveau de sécurité : c'est ce qu'offrent le WPA2/AES (cf. § 6.4.4).

6.2.4 Le déni de service

Empêcher le réseau de fonctionner

On pourrait croire, avec l'espionnage et l'intrusion, qu'on a fait le tour des attaques possibles. Mais il reste une catégorie d'attaques plutôt inquiétante : le déni de service (noté DoS). Le concept est simple : le pirate empêche le réseau de fonctionner normalement. L'exemple de déni de service le plus élémentaire (et le plus fréquemment cité comme exemple) est celui d'un pirate armé d'une hache, s'en allant tout bonnement réduire en miettes les AP de votre réseau.

Moins violent (et plus réaliste), un pirate peut attaquer votre réseau en émettant des ondes radio pour brouiller vos communications. S'il dispose du matériel nécessaire, qu'il émet à proximité, sur la bonne fréquence et avec un signal suffisamment puissant, vous ne pourrez plus rien émettre ni recevoir : votre réseau sera pour ainsi dire inutilisable.

Le déni de service a plusieurs buts possibles :

- le vandalisme gratuit ou intéressé (quand il est réalisé par un concurrent, par exemple) ;
- l'assouvissement d'une vengeance ;
- le pirate peut également demander une rançon pour rétablir le service. Cela s'est déjà vu avec des sites web très fréquentés : le pirate commence par le bombarder de requêtes *via* Internet au point que le site ne soit plus accessible, puis il envoie un message pour demander une rançon en échange de l'arrêt de l'attaque. Cependant, il est peu probable que des attaques similaires soient réalisées contre un réseau WiFi, car le pirate (ou en tout cas son matériel) doit obligatoirement se trouver à proximité physique du réseau : le risque de se faire prendre est assez élevé en comparaison d'une attaque *via* Internet ;
- le pirate peut faire une attaque DoS assez brève dans le but de déconnecter des utilisateurs pour les forcer à se reconnecter quelques instants après. Le but est alors d'essayer de subtiliser leurs mots de passe pour pouvoir faire plus tard une attaque d'intrusion.

Le déni de service n'a pas forcément lieu au niveau physique (à la hache ou avec les ondes radios) : il peut avoir lieu dans n'importe quelle couche réseau. Par exemple,

comme nous l'avons vu, il est possible de bombarder un site web de requêtes : c'est une attaque au niveau de la couche applicative. Dans le cas du WiFi, qui occupe les couches 1 et 2 du modèle OSI (voir les chapitres 2 et 3), les attaques de DoS possibles se situent donc au niveau de la couche physique et de la couche MAC.

Pour la couche MAC, une attaque consiste à émettre sans arrêt des paquets, pour saturer le réseau. Pire, absolument rien n'est prévu dans le standard WiFi pour sécuriser les paquets de gestion (tels que les trames balise, les trames d'authentification, de désauthentification, et les trames d'association et de désassociation), ni pour sécuriser les paquets de contrôles (paquets RTS, CTS, ACK...). Le groupe de travail 802.11w vise actuellement à combler ces lacunes.

> **Conclusion** : rien n'empêche à un pirate d'envoyer un paquet de désassociation à tous les utilisateurs connectés à un AP, en se faisant passer pour l'AP (un simple *spoofing* d'adresse MAC suffit). Les utilisateurs sont alors déconnectés de l'AP ! Autre option : le pirate peut sans arrêt envoyer des paquets CTS en se faisant passer pour l'AP : tous les utilisateurs croiront que l'AP a donné le droit à un autre utilisateur d'envoyer son paquet de données, et ils se mettront donc en attente.

Aucune solution

Autant le dire franchement : il n'existe aucune façon de se prémunir contre le DoS en WiFi, même avec les nouvelles solutions de sécurité. Le mieux que l'on puisse faire lors d'une attaque DoS est d'en trouver la source qui doit se situer non loin du réseau attaqué, et éventuellement d'appeler les autorités. Les concepteurs du standard ont estimé que, puisque ces attaques étaient toujours possibles au niveau physique[1], il n'était pas nécessaire de protéger la couche MAC. Pour la protéger aujourd'hui, il faudrait créer une nouvelle version de la norme 802.11 qui serait incompatible avec la norme actuelle. Malheureusement, il est beaucoup plus facile de réaliser une attaque au niveau MAC qu'au niveau physique : dans le premier cas, il suffit de disposer d'un adaptateur WiFi normal et d'un logiciel adapté (certains sont même disponibles gratuitement sur Internet), alors que pour une attaque physique, il faut un matériel spécifique, qui n'est pas à la portée de tout le monde. Ceci étant dit, dans les faits, l'attaque DoS des réseaux WiFi reste assez rare : cela s'explique sans doute par le fait que le pirate doit se situer à proximité, et que cela ne lui offre que peu d'intérêts.

> Il n'existe aucune façon de se prémunir contre une attaque de déni de service (DoS) en WiFi. Le mieux que l'on puisse faire est de mettre en place un mécanisme de détection, et de réagir dès qu'une attaque a lieu.

1. Dans d'autres technologies que le WiFi, il existe des méthodes pour éviter les attaques DoS au niveau physique : en utilisant la modulation FHSS (voir le chapitre 2) sur un spectre très large et en convenant d'une séquence pseudo-aléatoire de canaux sur lesquels on émet, il est très difficile pour un pirate de capter ou de brouiller le signal. Ces techniques sont bien sûr très appréciées par les militaires.

Pour finir sur les attaques DoS, il faut signaler que certains produits de supervision des réseaux WiFi, dont par exemple AirMagnet, permettent d'attaquer en DoS les réseaux pirates détectés. Si un employé branche un AP non sécurisé sur le réseau de l'entreprise, le matériel d'AirMagnet le détectera et l'attaquera pour empêcher qui que ce soit de s'y connecter, le temps que l'administrateur du réseau soit alerté et qu'il aille retirer *manu militari* l'AP pirate. Pour une fois qu'une attaque peut s'avérer utile pour la sécurité du réseau, il fallait le mentionner !

6.2.5 La modification des messages

La lettre remplacée

Un autre type d'attaque est la modification des messages échangés, à l'insu des interlocuteurs (fig. 6.4). On peut facilement voir les conséquences désastreuses que cela peut avoir : imaginez que votre lettre d'amour soit remplacée par une lettre d'insultes ! Un autre exemple, plus sérieux : imaginons qu'un employé souhaite effacer un fichier sur un serveur : il envoie alors une requête à ce serveur demandant à effacer le fichier choisi. À ce moment précis, un pirate intercepte la requête et parvient à la modifier en remplaçant le nom du fichier à effacer par un autre. On peut imaginer une foule d'autres exemples de ce type.

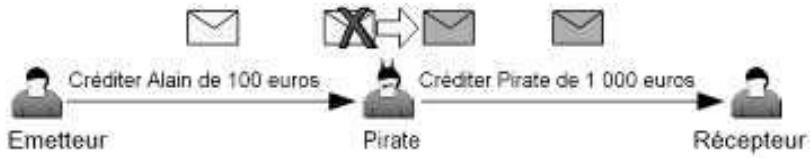


Figure 6.4 — Modification d'un message par un pirate.

Les attaques MiM

La modification des messages suppose que le pirate parvienne à s'interposer entre les interlocuteurs, à leur insu : on parle d'attaque de type *Man in the Middle*[1] (MiM, parfois noté MitM). Les attaques MiM peuvent aussi servir de base pour toutes les attaques décrites jusqu'à présent : espionner le trafic réseau, démarrer une nouvelle session, prendre le contrôle d'une session existante ou encore empêcher le réseau de fonctionner (DoS).

Une attaque MiM est bien sûr très facile à réaliser si le pirate a accès physiquement aux équipements du réseau. Par exemple, il peut intercaler son ordinateur entre un AP et le commutateur auquel cet AP est normalement connecté pour l'accès au réseau filaire. Par la suite, tous les paquets émis entre le réseau filaire et le réseau sans fil passeront par l'ordinateur du pirate, qui pourra alors à loisir espionner ou modifier ce que bon lui semble (fig. 6.5).

1. Littéralement : « Homme au milieu ».

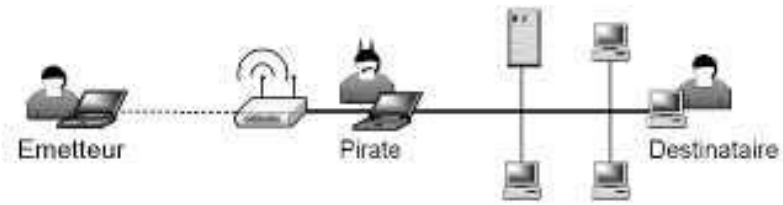


Figure 6.5 — Une attaque MiM simple.

De même, si un pirate peut se connecter au réseau sans fil, il peut en parallèle se faire passer lui-même pour un AP. Il lui suffit ensuite d'attendre qu'un utilisateur se connecte à lui (pensant qu'il s'agit d'un AP légitime) : par la suite, il peut servir d'intermédiaire entre le réseau et l'utilisateur (fig. 6.6).

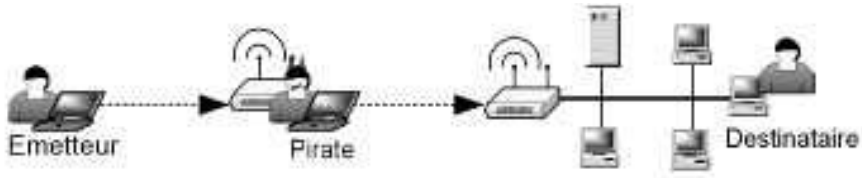


Figure 6.6 — Une attaque MiM en WiFi.

Il est plus difficile de mettre en œuvre une attaque MiM à distance, mais il existe tout de même des méthodes qui ont fait leurs preuves. La technique sans doute la plus utilisée exploite le fait que l'*Address Resolution Protocol* (ARP)[1] n'est pas du tout sécurisé.

Cette attaque est connue depuis longtemps, mais elle a connu un regain d'intérêt depuis l'arrivée du WiFi, car un pirate qui parvient à se connecter avec succès à un AP lui-même relié au réseau filaire peut lancer une attaque ARP contre n'importe quelle station, qu'elle soit connectée au réseau sans fil ou au réseau filaire (en tout cas si ces stations sont dans le même sous-réseau que le pirate). Cela signifie qu'il suffit qu'il y ait un seul AP non sécurisé relié à votre réseau pour qu'un pirate puisse espionner et modifier toutes les communications et pas uniquement celles du réseau sans fil (fig. 6.7) ! Pour en savoir plus sur l'attaque ARP, consultez l'annexe B sur *www.livrewifi.com*.

1. Pour un rappel sur les réseaux IP et leurs protocoles, consultez l'annexe A disponible sur le Web.

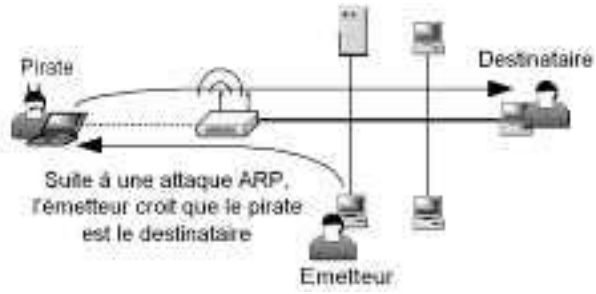


Figure 6.7 — Une attaque MiM contre une station du réseau filaire *via* le réseau sans fil.

Modifier un message crypté

Il est important de noter que le pirate n'a pas besoin de comprendre le trafic pour le modifier. En effet, même si chaque paquet de données est crypté, le pirate peut changer aléatoirement des bits et espérer que le message décrypté aura un sens pour le destinataire.

Cette stratégie n'est pas aussi absurde qu'elle en a l'air. En effet, certains algorithmes de cryptage ne changent pas l'ordre des bits, c'est-à-dire que le $n^{ième}$ bit du message crypté correspond au $n^{ième}$ bit du message original. C'est le cas en particulier de l'algorithme RC4 sur lequel reposent le WEP et le WPA comme nous le verrons au § 6.3.7 (en revanche, le WPA2 n'a pas ce défaut lorsqu'il repose sur l'algorithme AES). Par exemple, si le message original est « Bonjour Pat » et que le message crypté est « 9j3TdZ8Nai4 », alors on sait qu'en modifiant par exemple le dernier caractère du message crypté (ici le '4') par n'importe quoi, alors le dernier caractère du message décrypté par le destinataire sera également changé : « Bonjour PaL ». Ce sera le message original, sauf pour la dernière lettre qui pourrait être n'importe quoi. Bref, si l'on sait à quelle position dans le texte en clair se trouve l'information que l'on veut changer, il suffit de modifier le texte crypté à cet endroit précis. On ne pourra pas deviner ce que la modification donnera, mais on saura quelle partie du message on aura changé. Par exemple, le pirate peut supposer que le trafic repose sur TCP/IP (cas le plus fréquent) : il sait alors que le paquet de données commence par l'en-tête du paquet IP, et il sait donc à quel endroit précis il doit modifier le paquet crypté pour changer l'adresse IP de destination, par exemple. Cette attaque est à la base d'une des principales attaques contre le WEP, comme nous le verrons au prochain chapitre.

Nous avons vu au chapitre 3 (§ 3.6.1) qu'un code CRC (Contrôle de redondance cyclique) est rajouté à la fin de chaque paquet : il s'agit d'une sorte de résumé du paquet permettant de vérifier qu'il n'a pas été endommagé pendant son transport. Malheureusement, ce CRC a été conçu pour éviter les erreurs de transmissions, et non les modifications volontaires : il ne se trouve pas dans la partie cryptée des paquets. Du coup, rien n'empêche au pirate de modifier un paquet et de recalculer le CRC afin que le destinataire ne le rejette pas.

Nous verrons toutefois que le WEP, le WPA et le WPA2 offrent tous des mécanismes différents pour assurer l'intégrité des messages. Le mécanisme du WEP est malheureusement assez faible.

6.3 LES PREMIÈRES SOLUTIONS

6.3.1 Limiter les débordements

Une première mesure de protection contre les attaques du réseau sans fil consiste à s'assurer que les ondes radio ne débordent pas (ou peu) sur l'extérieur de l'entreprise. Ce n'est évidemment pas une énorme protection mais elle limite la tentation des curieux ou le fait que votre réseau figure dans les cartes de WarDriving sur Internet ! Cette protection doit être pensée au moment de l'audit de site et du déploiement, en positionnant correctement les AP pour que le niveau du signal soit très faible à l'extérieur des locaux.

6.3.2 Éviter les AP pirates

Même si votre réseau est parfaitement sécurisé, il suffit qu'un seul employé ait la mauvaise idée d'installer un AP non sécurisé et de le connecter au réseau filaire pour que toute votre sécurité soit anéantie. À ce sujet, il faut rappeler que l'une des principales raisons pour lesquelles les employés peuvent être tentés d'installer des AP pirates est qu'ils ne captent pas correctement le signal WiFi de votre réseau sans fil ou ne savent pas comment s'y connecter. Une façon de sécuriser votre réseau est donc de mettre en place un réseau WiFi de bonne qualité, avec une couverture dans l'ensemble des locaux et une capacité suffisante et d'informer correctement les employés.

> Déployer un réseau sans fil de qualité avec une bonne couverture, c'est réduire le risque qu'un employé soit tenté d'installer un AP pirate.

Il est également conseillé d'imposer des règles quant à l'utilisation des ondes radio au sein de l'entreprise. Par exemple, on pourrait imposer que le Bluetooth ne soit utilisé que pour synchroniser des PDA et jamais pour autre chose, afin d'éviter les interférences avec le WiFi (sauf bien sûr si l'on utilise le 802.11a ou le 802.11n à 5 GHz qui n'entrent pas en conflit avec le Bluetooth, comme nous l'avons vu).

6.3.3 La supervision radio

Il peut également être intéressant d'installer des sondes WiFi ou d'exploiter les fonctions de supervision radio offertes par certains AP, pour détecter les AP non sécurisés. La supervision radio peut permettre de détecter des AP non sécurisés, voire même certains types d'attaques WiFi, comme par exemple le spoofing d'adresse MAC ou certaines attaques DoS. Bien entendu, ce n'est qu'une mesure palliative, et non préventive : elle ne peut pas être utilisée seule.

Un réseau WiFi bien sécurisé est aussi un réseau bien supervisé.

6.3.4 Masquer le SSID

Comme nous l'avons vu au chapitre 3 (§ 3.5.1), il est parfois conseillé de masquer le SSID du réseau sans fil. Un passant équipé d'un matériel WiFi classique ne saura pas qu'un réseau sans fil se trouve à proximité ou en tout cas ne saura pas s'y associer facilement. Toutefois, il ne s'agit que d'une protection très faible, car il suffit de sniffer les ondes radio au moment où un utilisateur légitime se connecte : le SSID se trouve alors en clair dans sa requête d'association. En outre, chaque utilisateur légitime devra saisir manuellement le SSID du réseau sur son ordinateur. Bref, cette mesure apporte plus d'inconvénients que d'intérêts.

6.3.5 Le filtrage par adresse MAC

Un autre mécanisme pour repousser les « petits » pirates consiste à limiter l'accès au réseau sans fil à une liste d'équipements donnés, identifiés par leur adresse MAC (voir le chapitre 3, § 3.5.2). De nombreux AP disposent de cette fonction de filtrage par adresse MAC. Les adresses autorisées sont souvent stockées dans chaque AP, ce qui signifie qu'il faut modifier tous les AP lorsque l'on souhaite ajouter ou retirer une adresse MAC.

Le filtrage par adresse MAC a deux inconvénients majeurs :

- il est assez lourd à mettre en œuvre pour une moyenne ou grosse entreprise car il faut conserver la liste des adresses MAC de tous les équipements susceptibles de se connecter au réseau sans fil ;
- plus grave encore, il est assez simple pour un pirate de sniffer le réseau, de noter les adresses MAC d'utilisateurs légitimes, puis de « spoofer » (imiter) une adresse MAC légitime. Bref, cela ne sert qu'à arrêter les petits pirates et les simples curieux.

Avec ces deux inconvénients, on peut affirmer que le filtrage par adresse MAC ne vaut pas vraiment la peine d'être mis en œuvre.

6.3.6 Les VLAN

Si les AP le permettent (ou les commutateurs auxquels ils sont reliés), il est bon d'associer le trafic sans fil à un VLAN particulier. Ceci facilitera par la suite la maintenance et l'administration du réseau car tout le trafic provenant du réseau sans fil sera clairement identifié.

En outre, certains AP peuvent associer un utilisateur donné à un VLAN particulier au moment de l'identification (grâce au protocole RADIUS que nous étudierons au chapitre 10). Par exemple, lorsqu'un commercial se connecte au réseau sans fil, il peut automatiquement être associé au VLAN numéro 10 qui lui donne accès aux

serveurs généraux de l'entreprise ainsi qu'à des serveurs spécifiques aux commerciaux. Si un comptable se connecte, il peut être associé au VLAN numéro 20 qui lui donne accès aux serveurs généraux et aux serveurs réservés aux comptables. Enfin, si un simple visiteur se connecte, il peut être associé au VLAN numéro 30, lui donnant uniquement un accès limité et contrôlé à Internet.

Différentes politiques de qualité de service (QoS) peuvent être mises en œuvre sur les différents VLAN : un visiteur n'aura droit qu'à une très faible bande passante, alors que les commerciaux en auront suffisamment pour participer, par exemple, à des vidéoconférences.

6.3.7 Le cryptage WEP

Le WEP a pour objectif de protéger les communications WiFi en cryptant tous les paquets. Nous l'étudierons en détail au prochain chapitre.

Voici en deux mots le principe de son fonctionnement :

- tous les AP doivent être configurés avec une clé secrète, la « clé WEP », longue de 40 ou 104 bits[1] ;
- de même, tous les utilisateurs doivent configurer leurs adaptateurs WiFi avec cette même clé WEP ;
- par la suite, tout le trafic WiFi entre les utilisateurs et les AP est crypté. Le cryptage repose sur un algorithme appelé RC4 qui génère une série pseudo-aléatoire de bits. Ce « bruit » est en quelque sorte superposé au message, ce qui le rend illisible.

Première solution de cryptage à avoir été standardisée par l'IEEE, *Wired Equivalent Privacy* (WEP) signifie « sécurité équivalente au filaire ». Malheureusement, dans la pratique, la solution WEP ne s'est pas montrée à la hauteur de sa définition : à peine quelques mois après sa publication, des failles importantes ont été découvertes dans le WEP et exploitées presque immédiatement dans des attaques contre des réseaux WiFi. Des outils sont même disponibles gratuitement sur Internet qui permettent de casser la clé WEP, c'est-à-dire, en possédant suffisamment de paquets cryptés, de retrouver quelle clé WEP a servi au cryptage. Il suffit alors à un pirate de configurer son propre adaptateur avec cette clé WEP pour rendre le cryptage tout à fait inutile.

Le WEP a un autre problème majeur : tout le monde partage la même clé WEP.

Cela signifie que si la clé doit être changée, il faut le faire sur tous les postes et dans tous les AP. Ceci impose une énorme lourdeur de gestion. C'est d'autant plus grave que pour assurer une sécurité minimale, il faut changer la clé régulièrement, en particulier à chaque fois qu'elle risque d'avoir été compromise, ou lorsqu'un employé quitte la société. En outre, une seule indiscrétion d'un employé suffit à compromettre

1. Comme nous le verrons, la clé utilisée pour le cryptage est constituée de la clé WEP secrète précédée de 24 bits qui changent à chaque paquet envoyé, mais qui ne sont pas secrets. Néanmoins, pour des raisons commerciales, certains constructeurs d'AP parlent de clés WEP de 64 ou 128 bits.

la sécurité pour toute la société. Enfin, puisque tous les employés ont la même clé, rien n'empêche un employé mal intentionné d'espionner ou d'attaquer ses collègues.

Aujourd'hui, il est fort conseillé d'abandonner le WEP au profit du WPA ou du WPA2.

6.3.8 Isoler le réseau sans fil

On peut choisir de traiter les utilisateurs du réseau sans fil comme s'ils venaient d'Internet. Pour ce faire, on peut connecter les AP dans la DMZ (zone démilitarisée) de la passerelle d'accès à Internet ou simplement relier le réseau sans fil à une connexion à Internet complètement indépendante du réseau filaire. De cette façon, si un pirate parvient à se connecter au réseau sans fil, il ne pourra pas pour autant rentrer sur le réseau filaire (fig. 6.8).

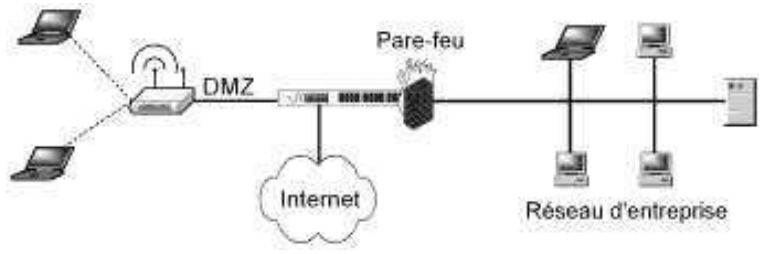


Figure 6.8 — Un réseau sans fil isolé du réseau de l'entreprise.

Cette stratégie est efficace pour protéger le réseau local, mais elle présente plusieurs inconvénients :

- pour les employés, le réseau sans fil ne sert qu'à accéder à Internet (ou à se connecter entre eux) : il n'est pas possible d'accéder au réseau filaire, à moins d'établir un tunnel VPN (voir le paragraphe suivant) ;
- les employés connectés sans fil sont en contact direct avec Internet et peuvent plus facilement être attaqués depuis Internet. Il faut donc installer un deuxième pare-feu (éventuellement intégré dans chaque AP) pour protéger les employés ;
- un pirate peut toujours attaquer les utilisateurs connectés au réseau sans fil. Pour éviter cela, certains AP peuvent être configurés pour interdire toute communication entre les utilisateurs sans fil. Malheureusement, les employés ne pourront plus communiquer entre eux. Cela n'empêche toutefois pas le pirate d'espionner les communications ;
- s'il parvient à s'associer à un AP, un pirate peut abuser de la connexion à Internet. Pour limiter ce risque, l'AP peut être relié à un pare-feu (encore une fois, il peut être intégré dans l'AP) et à un système de contrôle de la navigation Internet.

Cette isolation complète du réseau sans fil était parfaitement justifiée lorsqu'il n'existait pas de solution fiable pour sécuriser un réseau WiFi mais depuis l'apparition

de produits WPA et WPA2, l'intérêt est très limité. Néanmoins, si le réseau sans fil ne doit réellement être utilisé que pour accéder à Internet, alors cette architecture peut contribuer à protéger le réseau de l'entreprise.

6.3.9 Les réseaux privés virtuels

Des tunnels sécurisés

Pour permettre aux employés d'accéder tout de même au réseau de l'entreprise lorsque le réseau sans fil est isolé comme nous venons de le voir, il est possible de mettre en place un Réseau Privé Virtuel (RPV), plus connu sous le nom de *Virtual Private Network* (VPN).

Cela consiste à mettre en place un serveur VPN entre les AP et le réseau local. Il existe même des AP qui intègrent un serveur VPN, par exemple le CN1050 de la société Colubris Networks. Le serveur VPN permet aux employés de créer des « tunnels » de communication sécurisés, établis au niveau des couches 2 (L2TP) ou 3 (PPTP, IPSec...), voire dans des couches supérieures (SSH, SSL...).

Un employé commence par se connecter au réseau sans fil. À ce stade, il n'a pas encore accès au réseau local. Puis il exécute un logiciel (appelé le « client VPN ») qui établit une connexion sécurisée avec le serveur VPN, après identification de l'utilisateur. Par la suite, l'employé a accès au réseau de l'entreprise au travers du tunnel VPN, comme s'il était connecté directement au réseau filaire. En outre, l'ensemble de son trafic est crypté entre son poste et le serveur VPN (fig. 6.9).

Autre avantage, on peut éventuellement rendre le serveur VPN accessible depuis Internet et permettre ainsi aux employés de se connecter au réseau de l'entreprise pendant leurs déplacements (par exemple s'ils se connectent à des *hotspots*) ou depuis leur domicile. De nombreuses sociétés possèdent déjà un serveur VPN pour cet usage, ce qui évite d'avoir à en mettre un nouveau en place.

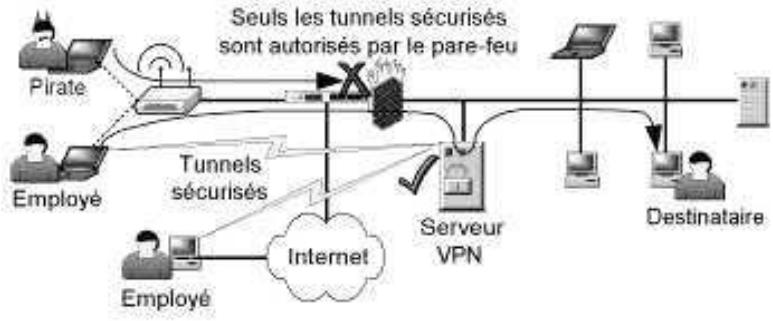


Figure 6.9 — La solution VPN.

Les défauts des VPN

Toutefois, isoler le réseau sans fil et obliger les utilisateurs à passer par des tunnels VPN pose quelques problèmes :

- les solutions VPN du marché peuvent coûter assez cher et sont parfois complexes à mettre en œuvre[1]. Il faut être très attentif à leur configuration pour éviter des failles de sécurité ;
- il faut bien choisir la solution VPN, car toutes n'offrent pas nécessairement un bon niveau de sécurité : la solution PPTP n'est pas considérée comme très robuste ;
- tout le trafic doit passer par un serveur VPN qui ne gère souvent qu'un nombre limité de connexions simultanées ;
- en passant par un tunnel VPN, le débit est parfois réduit et le temps de latence augmenté ;
- il n'est pas très pratique pour l'employé d'avoir à établir deux connexions (association WiFi puis connexion VPN) avant de pouvoir profiter du réseau.

Malgré ces défauts, la solution VPN était la seule à réellement offrir un niveau important de protection avant l'arrivée du WPA et du WPA2. Si votre matériel WiFi ne gère pas le WPA ou le WPA2 ou si vous avez déjà un VPN en place, cette solution est sans doute l'une des plus appropriées. Les réseaux VPN n'ont rien de spécifique au WiFi. De plus, mettre en place un réseau VPN est assez complexe et demanderait un ouvrage complet. Pour toutes ces raisons et sachant que le WPA et le WPA2 sont d'excellentes alternatives, nous ne détaillerons pas davantage les VPN.

6.4 LES NOUVELLES SOLUTIONS DE SÉCURITÉ

6.4.1 La mort du WEP

Même au moment de la conception du WEP, l'IEEE savait que cette solution était loin d'être parfaite, mais chacun pensait qu'elle serait suffisante pour satisfaire les besoins des utilisateurs pendant au moins quelques années. Après tout, cette solution reposait sur l'algorithme RC4 qui avait largement fait ses preuves. Ces quelques années devaient être mises à profit pour développer une nouvelle norme de sécurité plus robuste. C'est dans cette optique que le groupe de travail 802.11i, composé de nombreux experts en sécurité, commença à travailler : ils pensaient avoir beaucoup de temps devant eux. Malheureusement...

Dès sa publication, le WEP fut décortiqué sous tous les angles par les meilleurs experts en sécurité de la planète, et en moins de trois mois, il fut cassé. Cet échec retentissant fut largement relayé par la presse (à juste titre d'ailleurs). L'IEEE avait déjà commencé à travailler sur le 802.11i, mais fit comprendre qu'il faudrait encore attendre quelques années avant sa parution.

1. Il existe plusieurs solutions libres (Open Source), dont une connait un grand succès : OpenVPN.

6.4.2 Le LEAP et les solutions propriétaires

Pour les constructeurs de matériel WiFi, cette situation était inacceptable : certains se mirent donc à développer des solutions propriétaires. Il se trouve qu'un protocole à la mode à ce moment-là était le protocole d'authentification extensible (*Extensible Authentication Protocol*, EAP). Celui-ci définit un mécanisme assez générique, permettant d'identifier les utilisateurs qui cherchent à se connecter à un réseau, en restant très ouvert sur la méthode exacte d'identification : mot de passe, carte à puce, empreinte digitale ou tout autre mécanisme d'identification est possible.

C'est pourquoi Cisco choisit d'utiliser l'EAP pour sa solution de sécurité appelée *Lightweight EAP* (c'est-à-dire littéralement « EAP léger »). Cette solution fut la première à mettre en œuvre l'EAP en WiFi. Plus précisément, LEAP repose sur le protocole 802.1x, lui-même fondé sur l'EAP. Ce protocole suppose l'installation d'un serveur destiné à centraliser les mécanismes d'authentification des utilisateurs. Il s'agit presque toujours d'un serveur de type RADIUS.

6.4.3 Le WPA

La WiFi Alliance (l'association de constructeurs qui a défini le WiFi à partir du standard 802.11) décida alors qu'elle ne voulait ni attendre la parution du 802.11i, ni accepter que chaque constructeur définisse sa propre solution. Sa conclusion fut qu'il était nécessaire d'avoir rapidement au moins une version allégée du futur 802.11i. C'est ainsi qu'elle définit la solution *Wireless Protected Access* (WPA) : il s'agit d'une version allégée du standard 802.11i. Il existe deux variantes du WPA : le WPA Personal, également appelé *WPA-PreShared Key* (WPA-PSK) et le WPA Enterprise. Le WPA-PSK suppose la configuration d'une clé partagée dans tous les AP et équipements connectés au réseau. Le WPA Enterprise repose sur le protocole 802.1x et un serveur d'authentification RADIUS (à l'image du LEAP).

Le WPA repose sur le cryptage *Temporal Key Integrity Protocol* (TKIP) qui a été conçu de telle sorte qu'il soit possible de le mettre en œuvre dans les AP existants, par le biais d'une simple mise à jour de *firmware* (le microprogramme contenu dans l'AP). Tout en reposant encore sur l'algorithme RC4, comme le WEP, il corrige toutes les failles du WEP et peut être considéré comme très robuste. Toutefois, il n'a été défini que pour servir de transition vers le 802.11i, qui est la solution la plus sûre.

6.4.4 Le 802.11i (WPA2)

Le 802.11i permet d'utiliser un nouvel algorithme de cryptage, l'*Advanced Encryption Standard* (AES), qui est sans doute l'un des algorithmes les plus puissants aujourd'hui. Malheureusement, l'AES est plus exigeant en puissance de calcul que le RC4. Pour cette raison, un matériel plus performant est nécessaire pour le mettre en œuvre. Dès 2004, avant la parution du 802.11i, des AP assez robustes pour gérer l'AES ont vu le jour : dès la publication du 802.11i, en juin 2004, ils ont pu être mis à jour. Les AP antérieurs devront malheureusement être remplacés si l'on souhaite bénéficier de la meilleure solution de sécurité qui soit en WiFi.

Pour finir, on peut résumer les choses ainsi :

- le WEP n'est pas assez robuste et il a été cassé ;
- le LEAP fut novateur, mais c'est une solution propriétaire de Cisco ;
- le WPA est une version allégée du 802.11i conçue pour fonctionner avec le matériel existant. Il a été conçu pour assurer la transition vers le 802.11i. Deux architectures WPA sont possibles : WPA-PSK ou WPA Enterprise ;
- le 802.11i (WPA2) est la solution la plus sûre, mais elle suppose un matériel assez récent pour le gérer ;
- les solutions WPA Enterprise et WPA2 Enterprise reposent sur le protocole 802.1x, qui utilise lui-même le protocole EAP et suppose la mise en place d'un serveur RADIUS ;
- les solutions WPA Personal et WPA2 Personal reposent simplement sur une clé partagée entre tous les équipements du réseau.

Au cours des chapitres suivants, nous verrons précisément comment fonctionnent et comment mettre en œuvre le WEP (chapitre 7), l'EAP et le 802.1x (chapitre 8), le WPA et le WPA2 (chapitre 9) et enfin les serveurs RADIUS (chapitre 10).

Résumé

Pour conclure ce chapitre, passons rapidement en revue ce que nous avons appris :

– Un système d'information est sécurisé s'il assure la confidentialité et l'intégrité des données, ainsi que la disponibilité du système : on parle des qualités CID. Des mécanismes de non-répudiation peuvent également être mis en œuvre, mais pas au niveau du WiFi.

– Assurer la sécurité d'un système impose une vision globale et pas uniquement technique : cela implique de mettre en place une organisation de sécurité transversale et indépendante dans l'entreprise, de définir une politique globale, et d'assurer la sécurité à tous les échelons : en particulier aux niveaux organisationnel, humain, données, logiciels, réseau et physique. L'ensemble du système informatique doit être compartimenté et les droits des utilisateurs doivent être restreints pour éviter qu'une personne connectée au réseau, comme un visiteur ou même un employé, puisse tout faire.

– Le *wardriving* a mis en évidence l'importance de sécuriser les réseaux sans fil contre les attaques de réels pirates ou de simples curieux.

– Les attaques possibles contre un réseau WiFi peuvent être classées en quatre catégories : espionnage, intrusion, modification des données et déni de service. Les attaques de type relecture ou de type MiM peuvent servir à mettre en œuvre l'un des quatre types d'attaques fondamentales.

– Les parades possibles incluent : le cryptage des données échangées, un mécanisme fiable d'identification des utilisateurs, le contrôle rigoureux de l'intégrité des messages échangés, un mécanisme pour empêcher la relecture d'anciens messages. Tout cela est mis en œuvre dans le WPA et le WPA2 que nous étudierons dans les prochains

chapitres. Malheureusement, il n'existe aucune parade contre le déni de service au niveau WiFi, mais heureusement ces attaques sont rares car l'intérêt est limité et le pirate doit se situer à proximité du réseau sans fil.

– Des mesures de sécurité générales sont à mettre en œuvre, autant que possible : limiter le débordement radio, éviter les AP pirates, réaliser une supervision radio permanente et placer le réseau sans fil dans son propre VLAN.

– Beaucoup d'entreprises font le choix de sécuriser leur réseau WiFi à l'aide d'un VPN. Cela consiste à isoler le réseau WiFi (par exemple dans la DMZ) et à n'autoriser l'accès qu'à un serveur VPN ; une fois associée au réseau WiFi (sans contrôle) l'utilisateur n'a accès à rien tant qu'il n'a pas établi un tunnel avec le serveur VPN. Par la suite, tout son trafic passe par ce tunnel. Si votre entreprise a déjà une solution VPN en place, il n'est pas forcément intéressant de vous aventurer dans la mise en place d'une solution WPA Enterprise : votre VPN peut faire l'affaire.

– Quoiqu'il en soit, évitez la solution WEP qui est entièrement compromise comme nous le verrons au prochain chapitre.

– L'idéal est de mettre en œuvre une architecture WPA ou WPA2, avec une clé partagée (WPA Personal) à la maison ou avec un serveur RADIUS (WPA Enterprise) au bureau, ce que nous détaillerons dans les chapitres 8 à 10.

7

Le WEP

Objectif

Bien que de nombreuses failles, toutes plus graves les unes que les autres, aient été découvertes dans le *Wired Equivalent Privacy* (WEP), il s'agit encore aujourd'hui d'une solution utilisée dans de nombreuses entreprises. L'idéal est de mettre à jour ses équipements pour passer au WPA, voire au WPA2.

Ce chapitre a pour but de présenter rapidement les mécanismes et la mise en œuvre du WEP, entre autres pour vous convaincre de ses défauts, mais surtout pour mieux comprendre le WPA.

7.1 LA MISE EN ŒUVRE

7.1.1 Déployer le WEP

Le WEP, première solution de sécurité à avoir été intégrée dans le standard 802.11, suit un principe étonnamment simple : chacun doit connaître une même clé WEP, longue de 40 ou 104 bits et cette clé est utilisée par tous pour crypter les communications. Pour déployer une sécurité basée sur le WEP, en principe, rien de plus simple : il suffit de configurer chaque adaptateur WiFi (chaque ordinateur, chaque PDA, chaque AP) en y saisissant la clé WEP[1]. Pour plus de sécurité, il vaut mieux choisir la clé WEP aléatoirement.

1. Le standard ne précise rien quant à la façon d'installer la clé WEP dans chaque équipement. Dans la pratique, on doit la saisir manuellement.

La clé WEP peut en général être saisie de plusieurs façons différentes :

- au format hexadécimal : par exemple « F3-A9-20-E1-07 » pour une clé de 40 bits (5 octets), ou « 57-1A-00-FD-C1-AF-73-8C-21-0B-B3-A1-CD » pour une clé de 104 bits (13 octets) ;
- au format textuel : par exemple « P7n$i » pour une clé de 40 bits (5 caractères) ou « N1n?&Qw~@mBg8 » pour une clé de 104 bits (13 caractères). Le texte est alors converti en une séquence de bits grâce au codage ASCII : par exemple, la lettre « A » devient 01000001, c'est-à-dire 0x41 en notation hexadécimale ;
- certains adaptateurs permettent à l'utilisateur de saisir un mot de passe quelconque, par exemple « po9j3nmA ». Ce mot de passe est ensuite passé dans une « moulinette » propre à l'adaptateur, qui génère une clé WEP de 40 bits ou de 104 bits, au choix. Bien sûr, le même mécanisme doit être utilisé dans tous les équipements, ce qui suppose qu'ils soient tous du même constructeur. Si quelques équipements ne le sont pas, il faut récupérer la clé WEP générée automatiquement, et la saisir manuellement (par exemple au format hexadécimal) dans ces équipements.

Voilà ! La sécurité WEP est en place et toutes les communications sont cryptées. Ceci fonctionne autant en mode Infrastructure qu'en mode Ad Hoc. Les simples curieux ne peuvent plus se connecter facilement au réseau ou espionner ce qui s'y passe car il leur manque la clé WEP. Rien de bien compliqué, donc.

Figure 7.1 — Exemples d'interfaces de configuration de la clé WEP.

Malheureusement, les pirates motivés peuvent casser entièrement cette sécurité comme nous le verrons plus loin. En outre, chaque fois que l'on veut changer de clé WEP, il faut reconfigurer l'ensemble des équipements. Cette contrainte énorme pousse de nombreuses entreprises à choisir une clé WEP et à ne jamais la changer (ou très rarement). Ceci est très grave pour la sécurité du réseau.

7.1.2 La rotation des clés

L'un des problèmes avec le fait que tous les utilisateurs du réseau WiFi partagent la même clé WEP est que cette clé risque facilement d'être compromise : il suffit qu'un seul employé la divulgue pour que toute la sécurité soit réduite à néant. Il est donc important de la changer très régulièrement.

Le changement de clé WEP semble problématique : tout le monde doit-il modifier sa clé WEP en même temps ? Imaginez le cauchemar que cela peut représenter dans une moyenne ou grande entreprise ! Peut-on concevoir que tout le monde soit disponible au même moment pour configurer son ordinateur avec la nouvelle clé ? En parallèle, une batterie de techniciens devrait mettre à jour les clés WEP de tous les AP ? Et comment donner la clé WEP à tout le monde, d'un seul coup, sans compromettre cette clé ? L'envoyer par courrier électronique serait une solution peu sûre. Tout ceci est bien entendu inimaginable. Heureusement, l'IEEE a prévu ce point, et a défini un mécanisme pour faciliter le changement de clé WEP.

En réalité, le WEP autorise la définition de quatre clés, numérotées de 1 à 4. Dans chaque paquet crypté par le WEP, le numéro de la clé qui a été utilisée pour crypter le paquet est indiqué en clair, ce qui permet au récepteur du paquet de savoir laquelle des quatre clés il doit utiliser pour décrypter le message. Pour l'émission de paquet, une seule des quatre clés est utilisée : cette clé est appelée la clé « active ». Il faut bien comprendre que toutes les clés peuvent être utilisées à la réception, mais que seule la clé active est utilisée pour l'émission. Ceci permet de grandement faciliter le changement de clé WEP dans une entreprise.

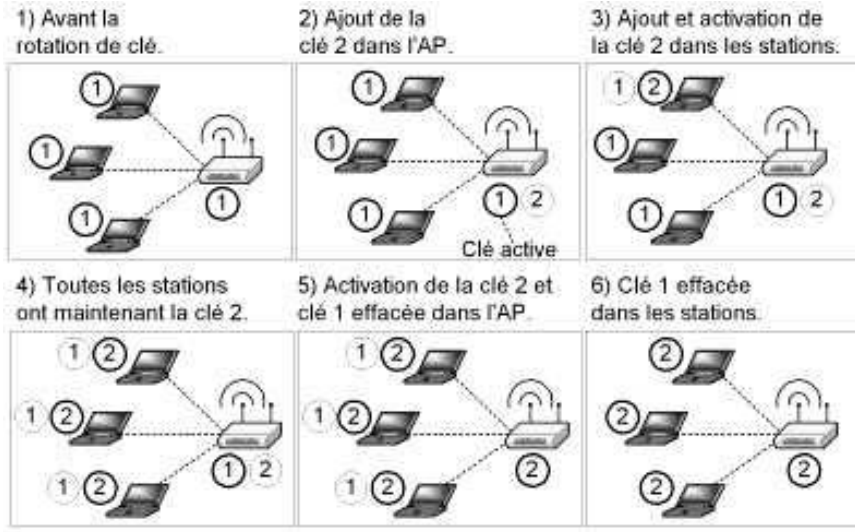


Figure 7.2 — La rotation de clé WEP.

Voici comment on peut procéder (fig. 7.2) :

- Au début, une seule clé est définie et active dans tous les équipements : par exemple, la clé numéro 1.
- Lorsque vous décidez de changer de clé WEP, il faut commencer par rajouter la nouvelle clé dans tous les AP : par exemple, à la position numéro 2. Toutefois, cette clé ne doit pas encore être activée : la clé numéro 1 est encore utilisée pour l'émission.
- Vous devez ensuite demander aux utilisateurs de rajouter la nouvelle clé WEP en position numéro 2, et de l'activer. Pour plus de sécurité, vous pouvez éventuellement demander à votre équipe de le faire, de sorte que seule votre équipe connaisse la clé WEP. Le temps que les postes de tous les utilisateurs soient mis à jour, il pourra s'écouler un certain temps, pendant lequel les AP recevront en partie du trafic crypté avec la clé numéro 1, et en partie du trafic crypté avec la clé numéro 2. Cela ne pose pas de problème car tous les AP connaissent déjà les deux clés et peuvent décrypter tous les paquets. En revanche, les paquets envoyés par les AP vers les utilisateurs sont toujours cryptés avec la clé numéro 1, qui est la seule connue de tous les employés, pour le moment.
- Une fois que l'on est sûr que tous les postes des employés ont bien été configurés pour utiliser la clé numéro 2, on doit se connecter à tous les AP pour activer cette clé numéro 2 et effacer la clé numéro 1 qui ne sert plus à rien.
- Pour plus de sécurité, on peut enfin demander aux utilisateurs d'effacer la clé numéro 1 de leur configuration.

Ce mécanisme permet d'assurer une transition « douce » d'une clé à une autre. Il n'en reste pas moins que cela suppose beaucoup de manipulations, et que c'est un système très pénible à gérer.

Par ailleurs, vous vous demandez sans doute pourquoi l'on peut définir quatre clés WEP, alors que deux semblent suffire amplement ? Nous allons voir cela tout de suite.

7.1.3 Les clés individuelles

Principe des clés individuelles

Le standard 802.11 définit deux types de clés WEP : la clé WEP partagée par tous (*shared key*) que nous venons d'étudier, mais aussi des clés WEP individuelles. Le principe des clés WEP individuelles est simple : chaque utilisateur dispose de sa propre clé WEP. Celle-ci est configurée et activée sur le poste de l'utilisateur, mais elle doit aussi être ajoutée dans tous les AP. Chaque AP contient, pour chaque utilisateur, sa clé WEP individuelle associée à son adresse MAC.

Lorsqu'un utilisateur envoie un paquet à un AP, il le crypte avec sa clé WEP individuelle. L'AP utilise l'adresse MAC de l'utilisateur (indiquée dans le paquet) pour savoir quelle clé WEP utiliser pour décrypter le paquet. De même, pour envoyer un paquet vers un utilisateur donné, l'AP utilise la clé WEP individuelle de cet utilisateur pour crypter le paquet.

On voit immédiatement quelle lourdeur ce mécanisme implique : dans une grande entreprise, il faudra que tous les AP contiennent la liste de toutes les clés WEP de tous les employés ainsi que leur adresse MAC ! Imaginez le temps que cela peut prendre de mettre en place un tel système pour une grande entreprise. À chaque fois qu'un employé intègre ou quitte la société, il faut se connecter à tous les AP et les reconfigurer pour rajouter ou ôter la clé WEP de l'employé en question.

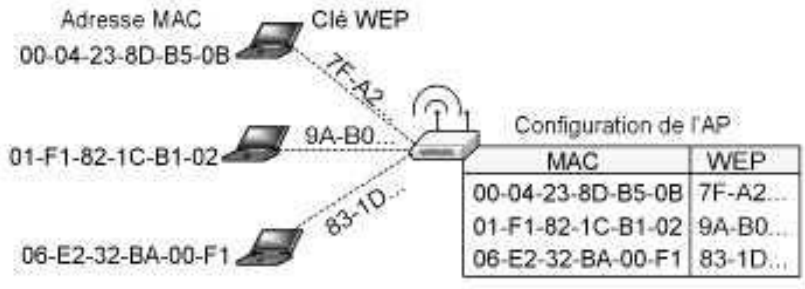


Figure 7.3 — Les clés WEP individuelles.

En revanche, les clés individuelles ont un avantage important : chaque employé possède sa propre clé, donc ses communications ne peuvent pas être espionnées par l'un de ses collègues. En outre, les clés individuelles ont moins de chances d'être divulguées qu'une clé WEP commune, connue de tous les employés. Le niveau de sécurité est donc plus important.

Le broadcast et le multicast

Il subsiste cependant un problème : que faire du trafic broadcast, c'est-à-dire les paquets envoyés à tout le monde ? Plus précisément, si un utilisateur veut envoyer un paquet à tout le monde, avec quelle clé WEP devra-t-il le crypter ? Avant de répondre à cette question, rappelons qu'en mode Infrastructure, comme nous l'avons vu au chapitre 3 (§ 3.2.1), chaque paquet émis par un utilisateur passe d'abord par l'AP auquel l'utilisateur est associé et cet AP se charge ensuite de relayer le paquet vers sa destination. En mode Infrastructure, le trafic broadcast proprement dit (diffusé vers tout le monde) est donc systématiquement émis par un AP, jamais directement par un utilisateur.

Cela réduit le problème du broadcast. En effet, puisque tous les paquets émis par un utilisateur passent par l'AP, qu'ils soient adressés à une seule station (unicast) ou à tout le monde (broadcast), l'utilisateur peut systématiquement utiliser sa clé WEP individuelle pour émettre les paquets. L'AP recevra le paquet crypté et saura le décrypter car il possède la clé individuelle de l'utilisateur. Reste ensuite à l'AP le rôle d'acheminer le paquet à destination.

Pour les paquets adressés à tout le monde, l'AP doit-il envoyer une copie à chaque utilisateur, individuellement ? Ce ne serait certainement pas efficace ! Pour cette raison, l'IEEE a décidé que pour le trafic broadcast émis par l'AP, une clé WEP partagée

(connue de tous) serait utilisée. Pour que tous les postes puissent recevoir et décrypter ce trafic broadcast, ils doivent donc connaître la clé WEP en question.

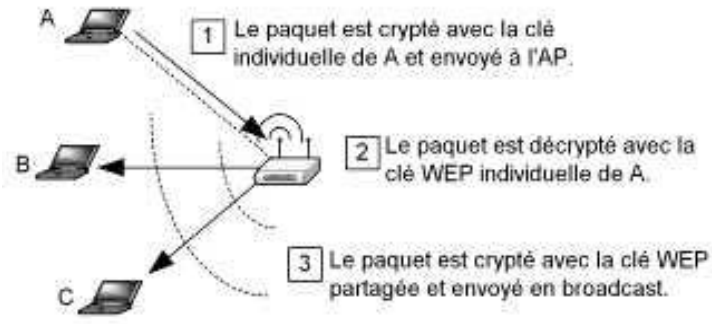


Figure 7.4 — Le cryptage du trafic broadcast.

Le même problème se pose pour le trafic multicast en général, c'est-à-dire pour les paquets envoyés à des groupes d'utilisateurs. La conclusion est la même que pour le broadcast : un utilisateur emploie sa clé individuelle pour envoyer un paquet en multicast, mais un AP utilise obligatoirement la clé partagée.

Configuration du réseau

Pour résumer, lorsque l'on décide de mettre en place une architecture WEP avec des clés individuelles, il faut :

- configurer chaque poste avec sa propre clé WEP individuelle, et l'activer : cette clé WEP sera donc utilisée pour crypter tous les paquets émis et pour décrypter les paquets reçus (sauf le trafic broadcast et multicast) ;
- configurer chaque poste avec la clé WEP partagée, mais ne pas l'activer : cela signifie que cette clé pourra uniquement servir à décrypter certains paquets reçus (en principe uniquement le trafic broadcast et multicast), mais pas les messages émis ;
- configurer tous les AP avec les clés WEP individuelles de chaque employé, associées aux bonnes adresses MAC ;
- configurer tous les AP avec la clé WEP partagée.

Dans cette architecture, chaque station a toujours au moins deux clés WEP à un moment donné : la clé partagée et la clé individuelle. Cela explique pourquoi l'IEEE autorise la définition de quatre clés : imaginez que vous souhaitiez à la fois changer la clé WEP partagée et les clés WEP individuelles en suivant le mécanisme de rotation de clé défini plus haut, vous voyez que quatre clés seront nécessaires pour assurer une transition douce : l'ancienne clé WEP partagée, la nouvelle clé WEP partagée, l'ancienne clé WEP individuelle et la nouvelle clé WEP individuelle.

Dans la pratique, la lourdeur de gestion des clés individuelles est telle que bien peu d'entreprises ont mis ce mécanisme en œuvre, malgré le léger gain de sécurité qu'il offre.

7.2 LES ROUAGES DU WEP

7.2.1 L'algorithme RC4

Le WEP repose sur un algorithme appelé RC4. Cet algorithme a été conçu par l'un des grands noms de la sécurité informatique : Ron Rivest. RC4 signifie d'ailleurs *Rivest Cipher 4* c'est-à-dire « Code de Rivest numéro 4 ». Pour information, Rivest est l'un des trois inventeurs de l'algorithme RSA (ce nom provient des initiales des inventeurs : Ron Rivest, Adi Shamir et Len Adleman).

L'algorithme RSA a révolutionné le monde de la sécurité informatique en introduisant le concept de clés asymétriques (voir l'annexe C, disponible sur le Web, *www.livrewifi.com*). En ce qui concerne le RC4, il est très utilisé aujourd'hui, en particulier dans toutes les transactions cryptées avec *Secure Socket Layer* (SSL), c'est-à-dire la quasi-totalité du commerce électronique. Il est également à la base du WPA sur TKIP, comme nous le verrons. RC4 a été le sujet de nombreuses études, et les meilleurs experts le considèrent comme très fiable. Cependant, même le meilleur outil peut être mal utilisé : c'est ce qui s'est passé avec le WEP.

> En soi, RC4 ne crypte rien : son rôle est de produire une série de bits pseudo-aléatoires. Pour cela, il faut lui fournir un point de départ, c'est-à-dire un certain nombre de bits quelconques qu'on appelle la « clé RC4 ».

En deux mots, RC4 fonctionne de la façon suivante : un tableau de 256 octets (donc 2 048 bits) est d'abord initialisé avec la clé RC4, répétée autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont réalisées : les octets sont déplacés dans le tableau, des additions sont effectuées, etc. Le but est de « mélanger » autant que possible le tableau. Au final, on obtient un tableau rempli d'octets très variés, qui paraissent tout à fait aléatoires. Par la suite, on peut continuer à mélanger ce tableau et en extraire des bits pseudo-aléatoires, au fur et à mesure. Les deux points importants à retenir sont les suivants :

- les séquences de bits produits par RC4 ont l'air parfaitement aléatoires ;
- on peut obtenir à nouveau exactement la même séquence de bits pourvu que l'on connaisse la clé RC4.

7.2.2 Crypter avec RC4

L'opération XOR

Pour comprendre comment WEP utilise RC4 pour crypter les paquets, il faut d'abord bien comprendre l'opération « ou exclusif », appelée également XOR (notée $\oplus$). Le

XOR est une opération très simple et très rapide qui se déroule au niveau de chaque bit : on peut le concevoir comme une addition binaire sans retenue. Ainsi :

$$0 \oplus 0 = 0 \qquad 0 \oplus 1 = 1 \qquad 1 \oplus 0 = 1 \qquad 1 \oplus 1 = 0$$

Si l'on applique le XOR sur une série de bits, on procède simplement bit par bit. Voici ce que cela donne pour un octet :

$$1001\ 0011 \oplus 1110\ 1001 = 0111\ 1010$$

En notation décimale, cela correspond à : $147 \oplus 233 = 122$. Un aspect très important du XOR est qu'en répétant la même opération deux fois, on revient à la valeur initiale : $a \oplus b \oplus b = a$. Donc, dans notre exemple, $147 \oplus 233 \oplus 233 = 122 \oplus 233 = 147$. Voyons maintenant comment tout ceci est exploité avec le WEP.

Procédure de cryptage

Une façon de crypter un message en utilisant RC4 est de réaliser un « ou exclusif » entre le message et la séquence de bits pseudo-aléatoires générée par RC4 : le message crypté est alors illisible pour un espion. Si le récepteur connaît la clé RC4 qui a été utilisée par l'émetteur, il peut générer à nouveau la même séquence pseudo-aléatoire et la combiner avec l'opération XOR au message crypté : il obtient ainsi le message original ! Résumons (fig. 7.5) :

- l'émetteur génère une séquence de bits pseudo-aléatoire R de même longueur que le message à envoyer : pour cela il utilise l'algorithme RC4 initialisé avec une clé RC4 ;
- il calcule le message crypté C à partir du message en clair M de la façon suivante : $C = M \oplus R$;
- il émet C, qui ressemble à une séquence de bits aléatoires ;
- à l'arrivée, on suppose que le destinataire connaît la clé RC4 qui a été utilisée par l'émetteur : il génère donc lui aussi la séquence de bits pseudo-aléatoire R à partir de cette clé ;
- pour retrouver le message en clair M, il calcule : $M = C \oplus R$.

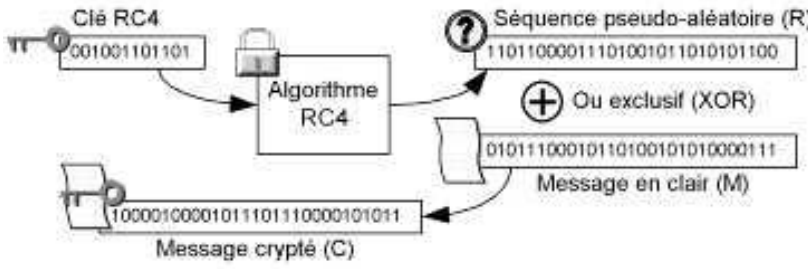


Figure 7.5 — Le cryptage RC4.

Notons que cette méthode n'est qu'une façon parmi d'autres d'utiliser RC4 pour crypter un message, mais c'est bien celle qui est employée par le WEP ainsi que par le WPA. En soit, il s'agit d'un cryptage assez sûr... mais alors, d'où viennent les vulnérabilités du WEP, et pourquoi le WPA est-il nettement plus robuste, alors qu'il repose sur le même mécanisme de cryptage ? Pour le comprendre, il faut aller un peu plus loin dans la compréhension des mécanismes du WEP.

7.2.3 Éviter la répétition de la clé RC4

Lorsque l'on doit envoyer plusieurs paquets de données, faut-il utiliser à chaque fois la même clé RC4 ? Si c'était le cas, cela voudrait dire que l'on utiliserait à chaque fois la même séquence pseudo-aléatoire pour crypter des paquets différents. En d'autres termes, pour envoyer deux messages distincts M_1 et M_2, on utiliserait dans les deux cas la même clé RC4 pour générer la séquence pseudo-aléatoire R. Cette séquence serait utilisée pour obtenir les messages cryptés C_1 et C_2, de la façon suivante :

$$C_1 = M_1 \oplus R$$

$$C_2 = M_2 \oplus R$$

Malheureusement, si un espion intercepte les deux messages cryptés, il peut alors réaliser l'opération suivante : $C_1 \oplus C_2$. Dans quel est l'intérêt ? Regardons cette opération de plus près :

$$C_1 \oplus C_2 = (M_1 \oplus R) \oplus (M_2 \oplus R) = (M_1 \oplus M_2) \oplus (R \oplus R) = M_1 \oplus M_2$$

On voit qu'en calculant $C_1 \oplus C_2$ l'espion parvient à éliminer R de l'équation ! Or ce R était ce qui donnait au message crypté son aspect aléatoire. À vrai dire, l'espion n'a pas encore les messages en clair, mais il n'en est pas loin. Pour vous en convaincre, admettons par exemple que le message M_2 soit entièrement rempli de zéros : dans ce cas, l'espion aura $M_1 \oplus M_2 = M_1 \oplus 0 = M_1$: le message M_1 lui apparaîtra en clair, comme par enchantement. Dans la pratique, il est peu probable que l'émetteur envoie des messages entièrement remplis de zéros, mais il arrive très fréquemment que des portions de messages soient nulles. Si le message M_2 contient des séquences nulles à certains endroits, cela laissera apparaître en clair des portions du message M_1, aux endroits correspondants. Et *vice versa* bien sûr. Dans la pratique, il existe même des méthodes statistiques pour automatiser le processus. Notez que la taille de la clé RC4 n'a aucune influence sur ce problème : une clé longue sera tout aussi vulnérable qu'une clé courte.

> Il faut éviter à tout prix de réutiliser la même séquence pseudo-aléatoire dans des paquets distincts.

7.2.4 Le vecteur d'initialisation

Une clé RC4 changeante

Pour éviter la répétition de la clé RC4, le WEP (et le WPA) utilise une solution très simple : pour chaque paquet, l'émetteur génère un numéro unique, qu'il ne réutilisera jamais (en principe). Un tel numéro est appelé un « *nonce* ». Une façon simple de générer des *nonce*s est d'utiliser une simple séquence (1,2,3,4...), mais chaque constructeur est libre de générer le *nonce* à sa guise. Ce *nonce* est combiné à une clé fixe pour créer la clé RC4 utilisée pour le cryptage du paquet. Avec le WEP, ce *nonce* est composé de 24 bits et s'appelle le vecteur d'initialisation *(Initialisation Vector*, IV). Il est simplement rajouté avant la clé WEP pour former la clé RC4.

La clé RC4 a donc le format suivant :

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

Bien entendu, pour pouvoir décrypter le message, le récepteur doit connaître la clé RC4 au complet. Il connaît déjà la clé WEP, puisqu'elle est configurée dans chaque poste et chaque AP du réseau, mais comment connaître l'IV ? La réponse est simple : l'IV est envoyé, en clair, au début de chaque paquet (après l'en-tête MAC).

Voici le format d'un paquet crypté avec le WEP :

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

Le champ ID indique laquelle des quatre clés WEP (de 0 à 3) a été utilisée pour le cryptage. Nous reviendrons sur le champ ICV plus loin, mais pour l'heure sachez juste qu'il fait partie du message crypté. Il suffit donc au récepteur de lire l'IV, de le rajouter avant la bonne clé WEP pour former la clé RC4, et à partir de là de décrypter le message.

> Le vecteur d'initialisation (IV) est un « *nonce* » (un nombre censé n'être utilisé qu'une seule fois) généré pour chaque paquet. Il est rajouté avant la clé WEP pour former la clé RC4 qui sert à crypter le paquet. Pour que le récepteur puisse décrypter le paquet, l'IV est envoyé avec le paquet.

Voilà, vous savez tout sur les mécanismes du cryptage WEP : ce n'est certainement pas le mécanisme le plus complexe qui soit, et il semble bien conçu au premier abord. Malheureusement, nous verrons plus loin qu'il est criblé de failles. Entre autres, l'IV est trop court : tôt ou tard, un même IV est réutilisé, donc la même clé RC4 sert à crypter deux paquets distincts, ce qui est très mauvais, comme nous l'avons vu. L'IV utilisé par le WPA est beaucoup plus long, ce qui permet de garantir que deux paquets

distincts n'utiliseront jamais la même clé RC4. C'est l'un des nombreux avantages du WPA sur le WEP.

7.2.5 L'authentification WEP

Nous avons vu au cours du chapitre 3 (§ 3.4.3) qu'avant de pouvoir s'associer à un AP, une station doit d'abord s'authentifier auprès de lui. Pour cela, elle envoie une requête d'authentification à l'AP. Cette requête ne contient aucune information d'identification de l'utilisateur (à part son adresse MAC, comme dans tout paquet WiFi) : elle correspond un peu à frapper à la porte d'une maison pour demander à y rentrer.

Si l'AP est en mode « ouvert » (*open system authentication*), alors il répondra positivement à toutes les requêtes d'authentification[1] : une fois que la station est authentifiée, elle peut demander à s'associer à l'AP.

En revanche, si l'AP est en mode d'authentification WEP (*shared key authentication*), alors il renverra un « défi » (*challenge*) à la station. Il s'agit d'une réponse contenant un texte de 128 caractères, généré aléatoirement. La station doit crypter ce texte avec le mécanisme WEP décrit plus haut, et renvoyer le résultat à l'AP. Celui-ci vérifie alors que le texte crypté est bien la version cryptée du défi : si c'est le cas, la station est considérée comme correctement authentifiée, et l'AP renvoie une réponse positive. Dans ce cas, la station peut ensuite s'associer à l'AP. Dans le cas contraire, bien sûr, la station reçoit une réponse négative et ne peut pas s'associer au réseau sans fil au travers de cet AP.

Encore une fois, ce mécanisme simple a été cassé, ce qui le rend tout bonnement inutile, voire même nuisible, comme nous le verrons.

7.2.6 Le contrôle d'intégrité

Le CRC

Le dernier volet de la sécurité WEP est le contrôle de l'intégrité des paquets échangés. Le but est de s'assurer qu'ils ne soient pas modifiés par un pirate pendant leur transport. Nous avons vu au chapitre 3 (§ 3.6.1) qu'un code de redondance cyclique (CRC) de 32 bits était rajouté à la fin de chaque paquet WiFi. Ce code est calculé en fonction du contenu du paquet et en constitue une sorte de résumé : si un pirate modifie ne serait-ce qu'un seul bit du paquet, le CRC ne sera plus valable. Malheureusement, le CRC a été conçu pour lutter contre les erreurs de transmission (et dans ce contexte il est efficace), mais il ne peut rien contre un pirate : en effet, si un pirate intercepte un paquet et le modifie, il lui suffit de recalculer le CRC avant de laisser ce paquet poursuivre sa route. Dans ce cas, le destinataire ne se rendra pas compte que le paquet a été modifié car le CRC sera correct.

1. À moins qu'un filtrage par adresse MAC ne soit réalisé.

L'ICV

Pour résoudre ce problème, le WEP a défini un mécanisme assez simple (fig. 7.6) : un code de vérification de l'intégrité du message (*Integrity Check Value*, ICV) est calculé de façon similaire au CRC habituel, sur 32 bits également. Toutefois, l'ICV est calculé non pas à partir du paquet « prêt à partir » (c'est-à-dire crypté) comme le CRC habituel, mais à partir du message original (en clair). L'ICV est inséré à la fin du message, et le tout est crypté par l'algorithme décrit précédemment.

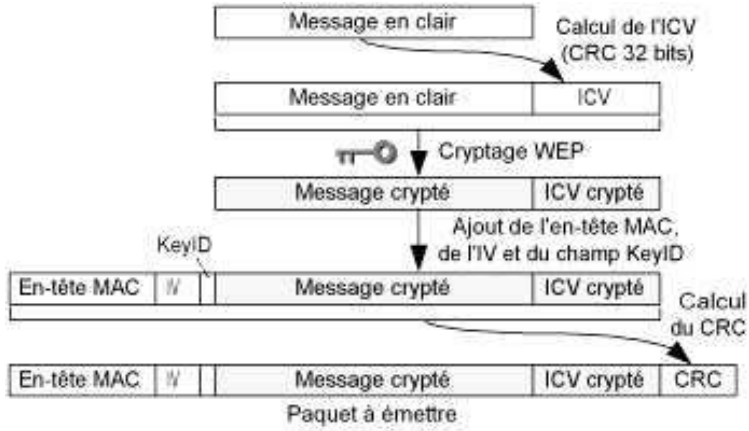


Figure 7.6 — Le contrôle d'intégrité avec l'ICV.

Pour préciser légèrement ce qui a été dit plus haut, si le message original est M et que la séquence pseudo-aléatoire générée par l'algorithme RC4 est R, alors le message crypté C est défini par la formule suivante :

$$C = [\, M \,||\, CRC(M) \,] \oplus R \qquad (\text{« || » signifie « suivi de »})$$

De cette façon, si un pirate veut modifier le paquet crypté, sans connaître la clé WEP, il aura en principe du mal à le faire. En effet, la modification donne un nouveau message crypté C', correspondant à un nouveau message en clair M'. Puisque le pirate ne possède pas la clé WEP, il ne peut pas savoir quel est ce message M' et ne peut donc pas calculer son ICV. Même s'il parvenait à le calculer, il ne pourrait pas le crypter pour l'intégrer à la fin du message C', car il ne possède pas la clé WEP.

Pourtant, aussi étonnant que cela puisse paraître, même ce mécanisme a été cassé, comme nous le verrons plus bas (c'est désespérant). Nous avons maintenant fait le tour de tous les mécanismes WEP. Il est temps maintenant d'en voir tous les défauts.

7.3 LES FAILLES

7.3.1 Les failles du cryptage

La répétition des clés RC4

Nous avons vu plus haut que si la même clé RC4 était réutilisée pour crypter plusieurs paquets, il était possible pour le pirate de retrouver le message d'origine. Le vecteur d'initialisation est censé éviter cela. Malheureusement, il n'est long « que » de 24 bits. Ceci peut paraître énorme car un nombre de 24 bits a 2^{24} = 16 777 216 valeurs possibles, soit presque 17 millions. Pourtant, admettons que le réseau sans fil soit utilisé modérément, par exemple avec un débit moyen de 1 Mb/s. Si les paquets ont une taille moyenne de 1 500 octets, par exemple, alors il est facile de calculer qu'il faudra moins de trois jours pour que soient envoyés 17 millions de paquets. Pour un réseau plus large et plus occupé, ce délai peut descendre à moins d'une heure !

Un pirate n'a donc qu'à attendre un temps somme toute assez limité pour obtenir des paquets dont l'IV est identique, donc qui ont été cryptés exactement avec la même clé RC4. Rappelons que pour obtenir ces paquets, il lui suffit de se placer à portée du signal radio, et d'utiliser un adaptateur en mode *monitor* : il peut alors « sniffer » tous les paquets, même ceux qui ne lui sont pas adressés.

L'IV est trop court (24 bits), et il est donc amené à être répété fréquemment.

Nous avons vu que deux paquets C_1 et C_2 cryptés avec la même clé RC4 sont vulnérables car $C_1 \oplus C_2 = M_1 \oplus M_2$. Le pirate peut donc retrouver M_1 et M_2, au moins en partie. En outre, la taille de la clé WEP utilisée (40 ou 104 bits) n'a aucune influence sur cette attaque. Cette attaque vous paraît grave ? Il y a bien pire...

Un dictionnaire de décryptage

Admettons que le pirate parvienne à connaître le contenu en clair de certains paquets cryptés (nous verrons ci-dessous comment il peut procéder) : il dispose alors de la version cryptée C et de la version en clair M. Il lui suffit de calculer $C \oplus M$ pour trouver la séquence de bits pseudo-aléatoires R qui a servi à crypter M. Comme il connaît également l'IV qui est indiqué en clair dans le paquet, il peut désormais utiliser R pour décrypter tous les paquets envoyés avec le même IV. Du moins, tous les paquets d'une taille inférieure ou égale à R : le pirate doit donc s'arranger pour que ces paquets connus soient aussi longs que possible. Nous y reviendrons.

Le pirate peut ainsi se constituer un dictionnaire contenant toutes les séquences pseudo-aléatoires correspondant aux IV déjà rencontrés. Une fois terminé, le dictionnaire a une taille inférieure à 30 Go, ce qui tient largement sur un disque dur. Dès lors, quand le pirate reçoit un paquet crypté, il lui suffit de regarder quel est son IV, et de trouver dans le dictionnaire la séquence pseudo-aléatoire correspondant à cet IV : elle lui sert alors à décrypter tout simplement le message. Notons que le pirate ne connaît pas la clé WEP elle-même, ni les clés RC4, mais il connaît toutes les séquences pseudo-aléatoires utilisées pour le cryptage, ce qui est tout aussi utile. Il

peut même générer lui-même ses propres paquets, correctement cryptés. En outre, tout ceci peut être automatisé : en quelques heures ou quelques jours, le pirate se constitue automatiquement son dictionnaire, et ensuite il accède au réseau comme un utilisateur légitime !

Reste à savoir comment le pirate peut connaître la version en clair de nombreux paquets. C'est ce que nous allons voir maintenant.

Les requêtes ping

Pour connaître le contenu en clair d'un paquet crypté par un AP, une excellente solution consiste à s'arranger pour envoyer une requête de type *ping* à une station du réseau. Un ping est une requête ICMP (voir l'annexe A disponible sur le Web) qui demande tout simplement à une autre machine de répondre par un écho de la requête. Par exemple, si l'on envoie à une station une requête ping contenant « abcd », elle renverra une réponse ping contenant également « abcd » (pourvu qu'elle accepte les requêtes ping). Si un pirate peut envoyer sans arrêt des requêtes ping à une station, il obtiendra en réponse une multitude de paquets dont le contenu en clair sera connu à l'avance, et qui auront été cryptés avec des IV différents ! C'est exactement ce dont le pirate a besoin pour constituer le dictionnaire décrit précédemment, et casser ainsi la sécurité WEP (fig. 7.7). Mais comment peut-il envoyer des requêtes ping s'il ne connaît pas la clé WEP ? C'est ce que nous allons voir maintenant.

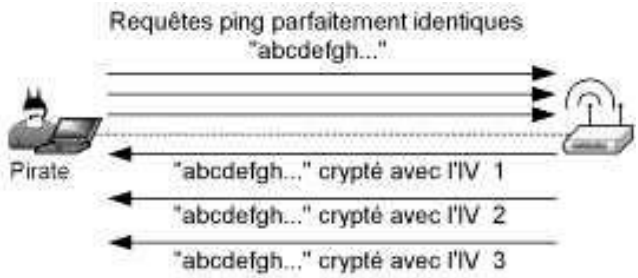


Figure 7.7 — Constitution d'un dictionnaire de décryptage grâce aux requêtes ping.

Relecture de ping

Pour pouvoir envoyer des requêtes ping, le pirate a une première option : il peut attendre qu'une requête ping soit envoyée par un utilisateur légitime du réseau. Il lui suffit alors d'enregistrer cette requête, puis de la répéter sans arrêt : puisque le WEP n'offre aucune protection contre la relecture (contrairement au WPA et au WPA2), le destinataire du paquet répondra tout à fait normalement.

Cependant, cette solution a deux inconvénients pour le pirate : d'une part, il aura du mal à reconnaître les requêtes ping, car elles sont cryptées. D'autre part, le pirate doit envoyer des ping contenant un maximum de texte, afin de pouvoir récupérer une séquence pseudo-aléatoire aussi longue que possible pour chaque IV. Or, un ping habituel est très court. Mais il y a mieux...

Fabriquer ses propres requêtes

Une meilleure option pour le pirate consiste à fabriquer lui-même ses propres requêtes ping. Voyons comment. Tout d'abord, il doit détecter un paquet envoyé par un utilisateur légitime, et dont le contenu est connu. Par exemple, il peut capturer une requête ARP (voir l'annexe A disponible sur le Web), facilement identifiable par sa taille : toujours 43 octets, si l'on compte l'IV (3 octets), l'en-tête LLC (8 octets), le paquet ARP (28 octets) et l' ICV (4 octets). Rappelons qu'une requête ARP est envoyée lorsqu'une station veut connaître l'adresse MAC d'une station dont elle connaît l'adresse IP. Son contenu est simple et facile à deviner. Le pirate possède donc le paquet crypté C, et sa version en clair M : il peut en déduire la séquence pseudo-aléatoire $R = C \oplus M$. Il connaît également l'IV, qui est en clair dans le paquet envoyé par l'utilisateur.

Dorénavant, puisqu'il possède un IV et la séquence pseudo-aléatoire correspondant à cet IV, le pirate est capable d'envoyer les paquets de son choix en les cryptant tout à fait normalement avec l'IV et la séquence pseudo-aléatoire qu'il possède. Toutefois, il n'a que les 43 premiers octets de cette séquence, donc il ne peut générer que des paquets d'une taille inférieure ou égale à 43 octets. Heureusement (pour lui), c'est suffisant pour envoyer une petite requête ping. Il peut ainsi envoyer des requêtes ping sur le réseau jusqu'à trouver une station qui réponde.

Allonger la séquence pseudo-aléatoire

Maintenant, le pirate va pouvoir chercher la suite de la séquence pseudo-aléatoire dont il dispose. Il commence par créer une requête ping longue de 44 octets. Comme il ne connaît que les 43 premiers octets de la séquence pseudo-aléatoire, il ne saura pas comment crypter le dernier octet. Qu'à cela ne tienne, il en choisit un arbitrairement, crypte le paquet avec la séquence pseudo-aléatoire de 44 octets ainsi obtenue et il l'envoie. Si l'octet choisi n'est pas le bon, le destinataire rejettera le paquet car l'ICV ne sera pas bon : c'est en effet l'ICV qui se situe à la fin du message crypté, comme nous l'avons vu. En revanche, si l'octet choisi est le bon, la station répondra bien au ping. Il suffit au pirate d'essayer tous les octets possibles (de 0 à 255), en attendant quelques instants entre chaque requête, jusqu'à ce qu'il reçoive une réponse. Dès lors, il connaît le 44^{e} octet de la séquence pseudo-aléatoire. Il peut recommencer la même procédure pour deviner le 45^{e} octet, puis le 46^{e} et ainsi de suite jusqu'à disposer d'une séquence pseudo-aléatoire d'une longueur égale au *Maximum Transmit Unit* (MTU) qui est la longueur maximale des paquets sur le réseau. Grâce à cette séquence, il peut désormais envoyer les paquets de son choix, et en particulier des requêtes ping aussi longues que possible ! Le tour est joué : il peut se constituer son dictionnaire.

Bien entendu, le pirate doit être prudent car il agit directement sur le réseau et il risque donc d'être repéré si l'on s'aperçoit, par exemple, que le débit diminue. Cependant, ceci est une technique automatisable qui casse entièrement la sécurité du WEP ! Pourtant, il existe une attaque encore bien plus rapide et efficace : l'attaque des clés faibles.

Les clés faibles

En août 2001, un article fut publié par Scott Fluhrer, Itsik Mantin et Adi Shamir (un autre des inventeurs de RSA, décidément) : *Weaknesses in the Key Scheduling Algorithm of RC4*. Cet article démontre qu'il existe une faiblesse dans l'algorithme RC4 : pour certains types de clés RC4, les premiers bits produits par l'algorithme ont une forte probabilité de correspondre à quelques bits de la clé ! Ces clés sont donc appelées des clés « faibles » (*weak keys*). Souvenez-vous que RC4 fonctionne en initialisant un tableau avec la clé RC4, puis en mélangeant et modifiant ce tableau. En somme, cet article montre que le tableau n'est pas tout à fait assez mélangé et modifié au moment où l'on commence à en extraire des bits, lorsque la clé RC4 est faible. Les attaques « FMS » (initiales des auteurs) profitent de cette faiblesse.

En soi, ce n'est pas un coup fatal contre l'algorithme RC4 : une solution simple consiste à jeter les premiers octets de la séquence pseudo-aléatoire, et la suite semble tout à fait imprévisible (il est recommandé de jeter les 256 premiers octets de la série produite).

Casser la clé WEP

Malheureusement, le cryptage WEP tombe dans la faille des clés faibles : en effet, ce sont avant tout les premiers bits de la clé RC4 qui déterminent si elle est faible ou non. Puisque l'IV est rajouté *avant* la clé WEP pour former la clé RC4 et que l'IV change tout le temps, on peut être sûr que l'on utilisera fréquemment des clés faibles.

Il suffit donc à un pirate de « sniffer » le réseau WiFi à la recherche de paquets cryptés avec des clés faibles. Puisque l'IV est envoyé en clair et qu'il correspond au début de la clé RC4 (qui détermine si une clé est faible ou non), il est facile de savoir si la clé utilisée pour crypter un paquet est faible ou non. Dès qu'il a capturé suffisamment de paquets cryptés avec des clés faibles, il utilise un algorithme (trop complexe pour être détaillé ici) qui permet de retrouver la clé WEP ! Cet algorithme prend un temps seulement proportionnel à la taille de la clé WEP, ce qui signifie que les clés de 104 bits ne sont qu'un peu plus de deux fois plus longues à casser que les clés de 40 bits. En d'autres termes, la taille de la clé WEP n'a que peu d'importance.

Cette attaque a plusieurs avantages sur la précédente :

- elle peut se faire sans agir sur le réseau, ce qui évite au pirate d'être détecté ;
- elle peut être beaucoup plus rapide car il suffit d'avoir un nombre suffisant de paquets cryptés avec une clé faible : sur un réseau très actif et avec un peu de chance on peut même craquer une clé WEP en moins de 10 minutes !
- à la fin, le pirate possède la clé WEP, et non un dictionnaire de 30 Go. C'est tout de même plus pratique.

Le seul inconvénient de cette attaque est qu'elle peut prendre beaucoup de temps si le réseau sans fil n'a pas beaucoup de trafic. Dans ce cas, elle peut être combinée à l'attaque précédente pour générer artificiellement du trafic sur le réseau.

S'il n'y avait qu'une faille à retenir, ce serait donc celle-ci : si un pirate peut trouver la clé WEP du réseau sans fil, tout le château de cartes s'écroule. Il peut déchiffrer

tous les messages. Il peut s'associer à l'AP, et envoyer lui-même des paquets. Il peut intercepter des paquets et les falsifier. Bref, si le pirate possède la clé WEP, le WEP ne vaut plus rien.

Peu de temps après la parution de cet article, des outils furent créés, mettant en œuvre cette attaque : AirSnort, WEPCrack et dweputils... disponibles gratuitement sur Internet !

Devant l'ampleur du désastre, des constructeurs ont réagi en créant des adaptateurs WiFi capables d'éviter les IV qui produisent les clés faibles. Rappelons en effet que l'émetteur peut choisir l'IV comme bon lui semble. Rien ne l'empêche donc d'éviter les IV produisant des clés faibles. Si tous les adaptateurs des stations du réseau évitent les clés faibles, alors cette attaque n'est plus possible. Malheureusement, en réduisant considérablement le nombre d'IV possibles, cela rend l'attaque précédente beaucoup plus rapide car les IV sont alors beaucoup plus rapidement réutilisés.

7.3.2 Les failles de l'authentification

Le mécanisme d'authentification WEP décrit plus haut comporte également une faille importante : une attaque de type MiM la rend parfaitement inutile. Voyons comment.

Le pirate peut configurer son ordinateur pour qu'il se comporte comme un AP. Ce n'est pas difficile à faire, en particulier sous Linux. Il fixe alors son SSID pour qu'il soit identique à celui du réseau sans fil qu'il souhaite attaquer. Dès lors, un utilisateur légitime passant à proximité risque d'être pris dans son filet, c'est-à-dire que son poste croira que l'AP du pirate fait partie du réseau. Le poste de l'utilisateur peut alors envoyer une requête d'authentification à l'AP du pirate, dans le but de s'y associer. Le pirate intercepte cette requête et envoie lui-même une requête d'authentification à un AP légitime. Cet AP répond au pirate en lui envoyant un défi, comme il se doit. Le pirate redirige ce défi vers l'utilisateur. Le poste de l'utilisateur, qui croit toujours qu'il parle à un AP légitime, répond au défi. Le pirate reçoit cette réponse et l'envoie à l'AP, en feignant qu'elle vient de lui. L'AP, voyant que la réponse est correcte, décide alors d'autoriser... le pirate ! Celui-ci peut ensuite tranquillement s'associer à l'AP, puisqu'il est authentifié. En parallèle, il peut arrêter de se comporter en AP : le poste de l'utilisateur recherchera alors automatiquement un autre AP et en trouvera un sans problème (sans doute le même que celui auquel le pirate est parvenu à s'associer). Ni l'utilisateur ni l'AP ne se rendent donc compte de quoi que ce soit.

Il est donc possible pour un pirate, par une simple attaque de type MiM, de contourner l'authentification WEP. En outre, le principe même de l'authentification WEP est absurde : il s'agit de prouver que l'on connaît bien la clé WEP, en répondant correctement à un défi. Mais à quoi cela sert-il, puisque de toute façon, si l'on ne connaît pas la clé WEP, on ne pourra pas communiquer avec le reste du réseau, une fois associé ? Ce mécanisme est donc parfaitement inutile. À une exception près : il permet à l'utilisateur qui ne dispose pas de la clé WEP (ou qui s'est trompé en la configurant) de savoir immédiatement qu'il a été rejeté par le réseau. Sans authentification WEP, il se retrouve associé à l'AP, avec l'impression que tout s'est bien déroulé. Mais au moment de communiquer avec le réseau, plus rien : tous les paquets émis ou reçus

sont rejetés. Avant de comprendre que le problème vient de sa clé WEP incorrecte, il peut perdre beaucoup de temps.

Mais l'authentification WEP a un autre inconvénient : elle donne aux pirates un exemplaire de texte en clair (le défi) et de sa version cryptée (la réponse au défi). C'est un indice de plus pour essayer de casser la clé.

Pour toutes ces raisons, bien que le standard 802.11 ait spécifié l'authentification WEP, la WiFi Alliance a décidé de l'interdire : les produits au label « WiFi », c'est-à-dire la grande majorité des produits 802.11, ne sont plus censés l'imposer. On ne trouve donc plus que l'authentification ouverte ! Tout le monde peut donc s'associer à n'importe quel AP, bien que cela ne signifie pas que cela lui donnera accès au réseau.

7.3.3 Les failles du contrôle d'intégrité

Le contrôle d'intégrité du WEP repose, nous l'avons vu, sur un code d'intégrité de 32 bits appelé l'ICV, calculé avec l'algorithme CRC à partir du message en clair et rajouté à la fin de ce message pour être crypté avec lui. Nous allons voir que ce mécanisme ne sert à rien.

L'algorithme CRC a une propriété assez intéressante : on dit qu'il est « linéaire ». Cela se traduit par la formule suivante :

$$CRC (A \oplus B) = CRC (A) \oplus CRC (B)$$

Cette propriété permet à un pirate de modifier un paquet crypté sans que le destinataire ne s'en aperçoive. Pour comprendre comment ceci est possible, il faut revenir à la définition du paquet crypté que nous avons vue plus haut : si le message en clair est M et la séquence pseudo-aléatoire générée par l'algorithme RC4 est R, alors le message crypté C est donné par la formule suivante :

$$C = [M \,||\, CRC(M)] \oplus R$$

Voyons ce qui se passe si le pirate modifie intelligemment le paquet crypté C pour obtenir un paquet modifié C'. Le pirate calcule C' en combinant C (*via* l'opération XOR) à une séquence Δ quelconque, de même longueur que M, suivie du CRC de Δ :

$$C' = C \oplus [\Delta \,||\, CRC(\Delta)]$$

En remplaçant C par sa définition, on obtient :

$$C' = [M \,||\, CRC(M)] \oplus R \oplus [\Delta \,||\, CRC(\Delta)]$$

Puisque M et ? ont la même longueur, que les deux CRC aussi ont la même longueur, et que l'opération XOR s'applique bit par bit, on trouve :

$$C' = [M \oplus \Delta \,||\, CRC(M) \oplus CRC(\Delta)] \oplus R$$

On y est presque : il reste juste à exploiter le fait que l'algorithme CRC est linéaire et l'on obtient :

$$C' = [\, M \oplus \Delta \,||\, CRC(M \oplus \Delta) \,] \oplus R$$

Si l'on note $M' = M \oplus \Delta$, on trouve :

$$C' = [\, M' \,||\, CRC(M') \,] \oplus R$$

Comme par magie, on voit que C' ressemble parfaitement à un paquet normal : pour s'en convaincre, il suffit de comparer ce résultat à la définition de C précédente. Du coup, C' sera tout à fait accepté par le destinataire, qui ne saura donc pas que le paquet aura été modifié par un pirate !

> **Résumons :** un pirate peut modifier comme il le souhaite n'importe quel paquet, et le mécanisme de contrôle d'intégrité du WEP n'est d'absolument aucun secours. Pour cela, il lui suffit d'appliquer la formule :
> $C' = C \oplus [\, \Delta \,||\, CRC(\Delta) \,]$

Le dernier rempart du WEP vient de s'écrouler. Avant de clore ce chapitre, rappelons tout de même que la solution WEP vaut mieux que de ne pas avoir de sécurité du tout : la plupart des attaques présentées précédemment ne sont pas réalisables par le premier venu. Il faut du temps, de la motivation et des compétences techniques, même si des logiciels gratuits facilitent considérablement la tâche du pirate. Néanmoins, il est fortement conseillé de mettre en place le WPA ou le WPA2, vous bénéficierez d'un niveau de sécurité incomparablement plus élevé.

Résumé

La solution de sécurité WEP est la première à avoir vu le jour, dès 1997, dans la norme 802.11. Elle est très simple à mettre en œuvre puisqu'il suffit de configurer chaque équipement avec une clé WEP de 40 ou 104 bits, saisie en général au format hexadécimal. Par la suite, toutes les communications sont cryptées grâce à cette clé WEP partagée. La même clé est utilisée dans tous les équipements, ce qui est loin d'être idéal, tant pour la sécurité que pour la maintenance : si la clé est compromise, il faut la changer dans tous les équipements.

Pour faciliter et encourager le changement fréquent de clé WEP, la norme 802.11 autorise que jusqu'à quatre clés WEP soient définies. Une seule est utilisée pour le cryptage (la clé « active ») mais toutes peuvent être utilisées pour le décryptage. Pour changer de clé WEP, il suffit donc de rajouter une nouvelle clé WEP dans tous les AP, sans l'activer, puis d'installer progressivement la nouvelle clé WEP dans toutes les stations, en l'activant et enfin d'activer la nouvelle clé WEP dans les AP.

Une clé WEP « individuelle » peut être installée et activée sur un poste. Il faut également la configurer dans chacun des AP, en l'associant à l'adresse MAC du poste en question. Lorsque l'AP reçoit ou envoie un paquet pour un pour un poste donné, il utilise la clé WEP individuelle de ce poste pour crypter ou décrypter le paquet. Ceci

permet d'améliorer la sécurité en évitant qu'une même clé soit utilisée par tout le monde pour leurs communications. Cependant, une clé partagée doit tout de même être installée pour le trafic broadcast et multicast.

Le cryptage WEP repose sur l'algorithme RC4 qui génère une série potentiellement infinie de bits pseudo-aléatoires à partir d'un point de départ : la clé RC4. Le cryptage WEP fonctionne simplement en combinant une séquence pseudo-aléatoire au message à crypter grâce à l'opération XOR (ou exclusif, noté $\oplus$). Celle-ci peut être vue comme une addition binaire sans retenue. La clé RC4 est constituée d'un vecteur d'initialisation (IV) de 24 bits, suivi de la clé WEP. L'IV change pour chaque paquet envoyé et est inséré en clair avant le message. Le récepteur peut ainsi, à partir de l'IV du paquet et de la clé WEP qu'il connaît, reconstituer la clé RC4, et à partir d'elle décrypter le message. Le numéro de la clé WEP à utiliser (de 0 à 3) est indiqué dans le paquet, juste après l'IV.

La solution WEP met également en œuvre un mécanisme censé garantir l'intégrité des paquets échangés, pour s'assurer qu'ils n'ont pas été modifiés par un pirate : l'ICV est calculé sur le message en clair (c'est un simple CRC de 32 bits) et rajouté à la fin du message pour être crypté avec lui.

Enfin, un mécanisme d'authentification peut optionnellement être mis en œuvre : avant de s'associer à un AP, une station envoie une requête d'authentification. Si l'authentification WEP est activée, l'AP répond par un défi : un texte aléatoire de 128 caractères, que la station doit crypter et renvoyer. L'AP vérifie alors que le texte crypté est le bon, et autorise ou non la station à s'associer.

Nous avons étudié plusieurs attaques possibles et conclu que tous les mécanismes de sécurité du WEP pouvaient être cassés par un pirate modérément compétent et motivé : le cryptage, l'intégrité et l'authentification sont tous vulnérables.

Pour conclure simplement, le WEP est mieux que rien, mais il faut dès que possible passer au WPA ou au WPA2.

8

Le 802.1x

Objectif

Jusqu'ici, nous avons décrit des mesures de sécurité assez faibles : éviter le débordement radio, détecter les AP pirates, masquer le SSID, filtrer par adresse MAC, utiliser le cryptage WEP, etc. Chacune apporte sa pierre à l'édifice, mais aucune ne constitue une véritable muraille contre un pirate motivé et compétent. Il est donc temps d'aborder le protocole EAP : il est à la base du 802.1x, sur lequel reposent à leur tour les nouvelles solutions de sécurité du WiFi, le WPA Enterprise et le WPA2 Enterprise[1].

Le but du protocole EAP est d'identifier et d'« authentifier ») les utilisateurs (c'est-à-dire vérifier leur identité) avant de les laisser rentrer sur le réseau. Nous commencerons par parler rapidement de son origine avant d'aborder son fonctionnement. L'une des beautés de ce protocole est qu'il est assez souple pour gérer de multiples méthodes d'authentification : mot de passe, carte à puce, certificats électroniques, etc. Nous présenterons donc les principales méthodes utilisées aujourd'hui, en mettant l'accent sur leurs avantages et inconvénients en termes de sécurité et de facilité de gestion.

Le protocole EAP peut être utilisé dans de multiples contextes, et le WiFi n'en est qu'un parmi d'autres. Ce chapitre ne comporte donc que peu d'allusions au WiFi, mais rassurez-vous, il est loin d'être hors sujet : comme nous l'avons dit, la sécurité du WPA Enterprise et du WPA2 Enterprise dépend directement d'EAP. Si vous mettez en œuvre une méthode d'authentification EAP offrant peu de sécurité, alors votre protection WPA ou WPA2 ne vaudra pas grand-chose.

1. Le WPA Personal et le WPA2 Personal reposent sur une simple clé partagée, ils n'utilisent donc pas les mécanismes d'authentification du 802.1x.

8.1 L'ORIGINE D'EAP

Le protocole d'authentification EAP (*Extensible Authentication Protocol*) a été défini par l'*Internet Engineering Task Force* (IETF). Avant de parler d'EAP, un petit mot sur l'IETF s'impose.

8.1.1 L'IETF

Au cours des chapitres précédents, nous avons déjà parlé maintes fois de l'IEEE, qui a standardisé un grand nombre de technologies liées aux réseaux et à l'électronique, à commencer par le WiFi. Mais nous n'avons pas encore mentionné l'IETF. Or, l'IETF a standardisé la plupart des protocoles qui régissent l'Internet, à commencer par IP, PPP, HTTP et bien d'autres encore, dont la plupart des protocoles dont nous allons parler dans ce chapitre.

L'IETF est un organisme atypique : informel et auto-organisé, il ne s'agit ni d'une association, ni d'une société privée, ni d'un organisme gouvernemental. En principe, n'importe qui peut proposer un nouveau protocole à l'IETF : il s'agit de proposer un document définissant précisément ce protocole, en suivant une nomenclature assez stricte. À ce stade, il s'agit d'un *draft*, c'est-à-dire un brouillon. Après de nombreuses relectures, un travail de peaufinage méticuleux, et si le document est considéré comme assez sérieux, il est promu au rang de *Request For Comments* (RFC), c'est-à-dire littéralement « demande de commentaires ». Vous pouvez librement émettre des commentaires et suggérer des améliorations. Parfois, suite aux commentaires, une nouvelle RFC est créée, et rend la précédente obsolète. C'est ainsi, par exemple, que l'EAP a été défini dans la RFC 2284. En juin 2004, elle a été remplacée par la RFC 3748 qui lui a apporté quelques corrections et de nombreuses précisions, notamment concernant la sécurité.

Après parfois de longues années, une ou plusieurs RFC peuvent être intégrées dans un véritable standard. Ceci dit, de nombreuses RFC sont utilisées bien avant d'être officiellement standardisées. De même, certains *drafts* ont du succès. Il ne faut cependant compter que sur les plus stables d'entre eux, et surtout ceux qui ont le plus de chance de devenir un jour des RFC.

Toutes les RFC (ainsi que les *drafts* les plus sérieux) sont publiées sur le site web de l'IETF (*www.ietf.org*), aussi nous vous invitons à y jeter un coup d'œil : malgré leur apparence austère, les RFC sont en fait assez lisibles... si l'on parle anglais, bien sûr ! Il existe heureusement des traductions en français de nombreuses RFC[1].

8.1.2 Le protocole PPP

Le 802.1x est une pyramide de protocoles dont la base est l'EAP. Pour comprendre le 802.1x, il faut donc comprendre l'EAP. Et pour bien comprendre l'EAP, il faut

1. En particulier sur le site *http://abcdrfc.free.fr/*.

revenir à son origine : si vous avez déjà lancé une connexion à Internet *via* un modem téléphonique classique[1], votre ordinateur a commencé par établir une connexion avec une sorte de central téléphonique composé d'une batterie de modems eux-mêmes reliés à Internet (fig. 8.1). Ce central, mis en œuvre par un Fournisseur d'Accès à Internet (FAI), s'appelle un point de présence (*Point of Presence*, PoP). La connexion entre votre modem et l'un des modems du PoP repose sur un protocole très répandu : le Protocole de Point à Point (*Point-to-Point Protocol*, PPP), décrit dans la RFC 1661 et quelques RFC associées.

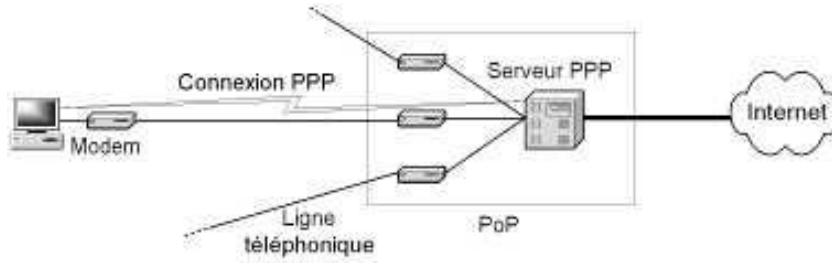


Figure 8.1 — Une connexion RTC avec le protocole PPP.

Le PPP définit notamment comment vous devez vous identifier : un mot de passe vous a été attribué par votre FAI, et vous devez simplement prouver que vous le connaissez. Si c'est le cas, le PoP vous laisse passer vers Internet, sinon, vous recevez un refus catégorique et la connexion est interrompue.

8.1.3 L' authentification avec PPP

Passons en revue les quatre principales méthodes d'authentification par mot de passe prévues par le PPP.

PAP

Le *Password Authentication Protocol* (PAP) est défini dans la RFC 1334. Il s'agit sans doute du plus simple des mécanismes d'authentification : le client envoie son mot de passe, en clair, c'est-à-dire non crypté ! Dans la pratique, le PAP est si peu sûr qu'il n'est utilisé que lorsqu'un autre mécanisme permet d'assurer la sécurité de l'échange.

CHAP

Le protocole *Challenge Handshake Authentication Protocol* (CHAP) est défini dans la RFC 1994. Le serveur commence par envoyer un « défi » au client (16 octets aléatoires), ainsi qu'un compteur qu'il incrémente à chaque fois qu'il lance un défi (fig. 8.2). Le client doit alors passer le compteur, son mot de passe et le défi au travers d'un algorithme de hachage, habituellement l'algorithme MD5[2]. Le résultat est une

1. On parle de connexion RTC (Réseau téléphonique commuté).
2. MD5, défini dans la RFC 1321, est un algorithme conçu (encore une fois) par Ron Rivest.

séquence de bits pseudo-aléatoires qu'on appelle le « *hash* » (de 16 octets dans le cas de MD5). Ce *hash* est envoyé au serveur, qui peut alors effectuer le même calcul et vérifier si son résultat concorde avec celui du client. Cet algorithme permet d'éviter que le mot de passe ne soit transféré et évite également qu'un pirate ne répète simplement une authentification réussie qu'il aurait enregistrée auparavant, puisque le défi change à chaque authentification. Il ne permet cependant pas au client de s'assurer de l'identité du serveur.

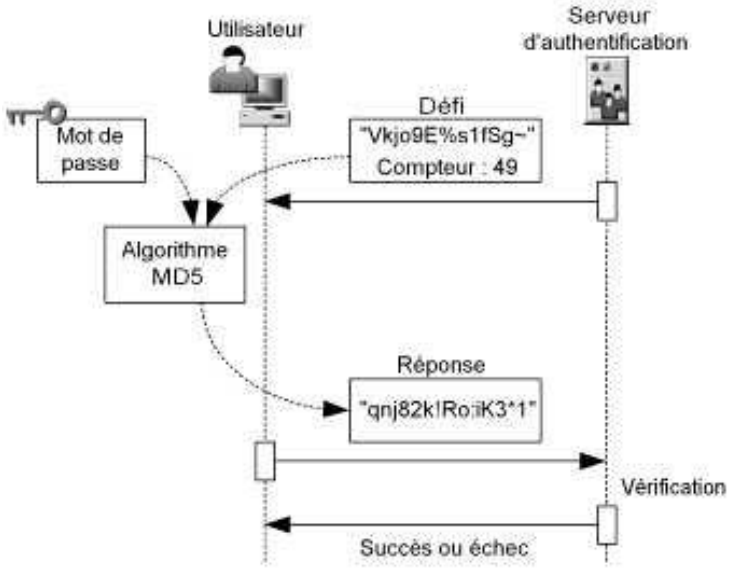


Figure 8.2 — L'identification avec le protocole CHAP.

MS-CHAP

Ce protocole, souvent appelé MS-CHAP-v1, a été défini par Microsoft dans la RFC 2433. Il s'agit d'une variante de CHAP, destinée à en améliorer la sécurité. L'un des problèmes de CHAP est le fait qu'il soit nécessaire de stocker le mot de passe en clair sur le serveur[1] : sinon, impossible de calculer le *hash* et de vérifier l'identité du client. Toute personne ayant accès à la base de données des utilisateurs peut donc voir les mots de passe de tout le monde ! Pour éviter cela, MS-CHAP spécifie que le serveur doit stocker non pas le mot de passe, mais le résultat d'un *hash* sur ce mot de passe (selon un algorithme propriétaire de Microsoft). Lorsque l'utilisateur saisit son mot de passe, celui-ci doit d'abord être passé au travers du même algorithme de *hash* avant de suivre la procédure habituelle de CHAP. Malheureusement, MS-CHAP comporte des failles de sécurité (dues en particulier au *hash* propriétaire de Microsoft) qui l'ont rendu rapidement obsolète : seuls quelques vieux systèmes Windows 95/98 l'utilisent encore.

1. Ou en tout cas de telle sorte que l'on puisse facilement récupérer le mot de passe en clair.

MS-CHAP-v2

Suite à la découverte des failles de sécurité dans MS-CHAP, Microsoft a réagi en concevant cette version 2, définie dans la RFC 2759. Nettement plus robuste, ce protocole fournit notamment un mécanisme d'authentification mutuelle : le serveur s'assure de l'identité du client et *vice versa*, ce qui n'est pas le cas avec les méthodes d'authentification précédentes. Le MS-CHAP-v2 est largement utilisé dans les réseaux Windows, depuis la version Windows 2000.

Les limites de ces méthodes

Tout cela fonctionne donc très bien. Malheureusement, la méthode PAP n'est pas sécurisée et les méthodes CHAP, MS-CHAP et MS-CHAP-v2 sont toutes vulnérables face à des attaques hors-ligne de type dictionnaire : si un pirate peut enregistrer les échanges lors de l'authentification d'un utilisateur légitime, alors hors-ligne (c'est-à-dire chez lui, déconnecté du réseau), il peut essayer de reproduire le même dialogue en essayant des milliers de mots de passe. Il suffit qu'un seul utilisateur légitime ait un mot de passe faible pour que le pirate puisse entrer sur le réseau.

En outre, certains FAI ont estimé qu'il était dommage qu'on ne puisse identifier les utilisateurs que sur la base d'un simple mot de passe. Certains voulaient pouvoir identifier les utilisateurs avec une carte à puce, d'autres voulaient utiliser des certificats électroniques, etc. C'est de ce besoin qu'est né l'EAP.

8.2 LE FONCTIONNEMENT D'EAP

8.2.1 L'architecture : trois acteurs

Une vue d'ensemble

Le principe d'EAP est très simple : si un client (c'est-à-dire un utilisateur) cherche à accéder au réseau, un contrôleur d'accès lui barrera le chemin jusqu'à ce qu'il s'identifie auprès du serveur d'authentification[1]. Le contrôleur d'accès sert d'intermédiaire pour la communication entre le client et le serveur d'authentification. Il n'a pas besoin de comprendre quoi que ce soit à cette communication, à l'exception du résultat final (le succès ou échec de l'authentification) qui le décidera à ouvrir la porte du réseau ou à la laisser fermée. S'il l'ouvre, l'ensemble du trafic du client vers le réseau passera par lui. Dans le cadre du WiFi, lorsque le 802.1x est utilisé, chaque AP est un contrôleur d'accès (fig. 8.3).

1. La terminologie peut devenir assez confuse car les protocoles EAP, 802.1x et RADIUS ont tous des mots différents pour désigner les mêmes choses. Par exemple, le client s'appelle respectivement *peer*, *supplicant* et *user* dans ces trois protocoles. De même, le contrôleur d'accès s'appelle *authenticator* dans l'EAP et le 802.1x, mais *Network Access Server* (NAS) ou *client* dans le RADIUS. Pour parfaire la confusion, *authenticator* signifie tout autre chose dans le RADIUS !

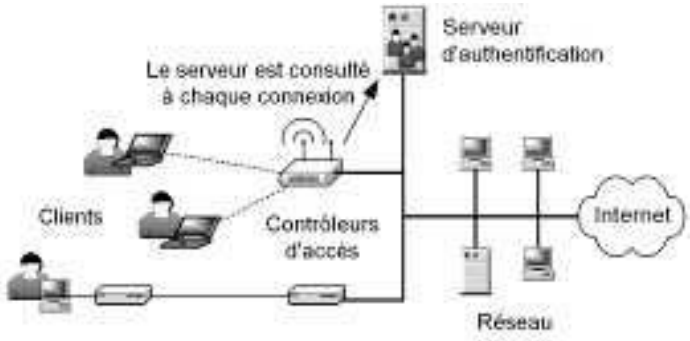


Figure 8.3 — Vue d'ensemble du protocole EAP.

Voici une petite analogie qui vous aidera peut-être à mieux vous représenter EAP : le contrôleur d'accès est un gardien musclé, mais pas très brillant. Lorsqu'un visiteur veut rentrer, le gardien demande au patron (le serveur d'authentification) ce qu'il faut lui dire. Il répète ensuite au visiteur, mot pour mot, ce qu'a dit le patron. Si le visiteur donne un mot de passe ou fournit des informations quelconques, le gardien répète tout au patron, sans réfléchir. Mais lorsque le patron dit enfin que le visiteur peut rentrer, le gardien comprend, et il laisse rentrer le visiteur.

Le fait que le contrôleur d'accès ne soit qu'un intermédiaire entre le client et le serveur est l'un des grands intérêts de l'EAP : en effet, si l'on invente une nouvelle méthode d'authentification, il ne sera pas nécessaire de changer les contrôleurs d'accès, car seuls les clients et le serveur d'authentification devront être mis à jour. En outre, les contrôleurs d'accès sont parfois de simples équipements sans grande puissance de calcul ou difficiles à mettre à jour, et il est bon que leur rôle se limite à servir d'intermédiaire.

> Lors de l'authentification EAP, le contrôleur d'accès n'est qu'un simple intermédiaire entre l'utilisateur et le serveur. Dès que l'utilisateur est bien authentifié par le serveur, le contrôleur d'accès le laisse passer vers le réseau.

Un exemple de configuration

Pour illustrer l'architecture EAP, voici un exemple de configuration possible dans un contexte WiFi (fig. 8.4) :

- Le client possède un logiciel de connexion fourni avec son adaptateur WiFi. Ce logiciel est compatible avec le 802.1x (donc avec l'EAP) et supporte deux méthodes d'authentification : PEAP/MS-CHAP-v2 et EAP/TLS (nous les décrirons dans les paragraphes suivants).
- Le contrôleur d'accès est un AP compatible 802.1x : il n'a pas besoin de connaître PEAP/MS-CHAP-v2, EAP/TLS ou toute autre méthode d'authentification particulière. Il est toutefois capable de relayer des requêtes EAP vers le client (*via* la connexion WiFi) et vers le serveur d'authentification (*via* le réseau de l'entreprise).

- Le serveur d'authentification est un serveur RADIUS compatible avec EAP. Il gère les méthodes d'authentification EAP/TLS et TTLS/PAP (voir paragraphes suivants). Le serveur demandera au client de s'identifier selon une méthode. Si le client ne la gère pas, le serveur en suggérera une autre et ainsi de suite jusqu'à ce que le client en accepte une. Dans cet exemple, ils tomberont d'accord sur la méthode d'identification EAP/TLS.

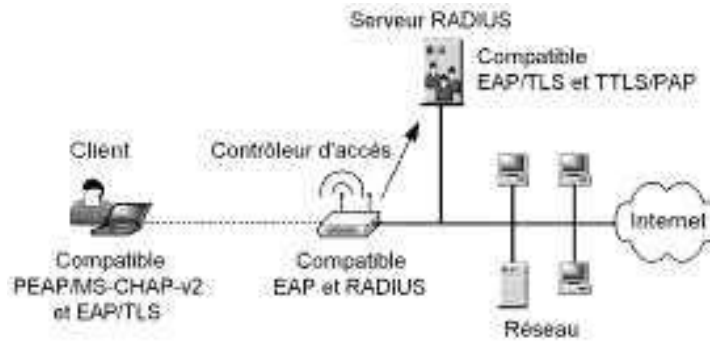


Figure 8.4 — Un exemple de configuration EAP.

Cet exemple illustre une configuration possible, parmi bien d'autres.

> Lorsque l'on décide de mettre en place une architecture qui repose sur l'EAP, il faut choisir les méthodes d'authentification que le serveur acceptera, et s'assurer que chaque client soit bien compatibles avec au moins l'une de ces méthodes.

Le logiciel client

Le logiciel de connexion du client (appelé le « client EAP ») peut être fourni avec l'adaptateur WiFi. Il peut également être acheté auprès d'un éditeur de logiciels : par exemple, *Odyssey Client* de la société Funk Software, ou *Aegis Client* de Meetinghouse. Il existe également des logiciels Open Source, comme *Xsupplicant*, pour Linux.

Le client EAP peut aussi être intégré au système d'exploitation. Windows possède ainsi un client EAP capable de gérer de multiples méthodes d'authentification pour toutes vos connexions réseau (filaires ou non). De même pour Mac OS.

Il est important de prendre le temps de bien choisir le client EAP, en fonction bien sûr de son coût, mais aussi de son ergonomie, sa stabilité, les méthodes d'authentification qu'il est capable de gérer, son ouverture (Open Source ou non), la qualité du support disponible, et les plates-formes sur lesquelles il peut fonctionner.

Voici un petit résumé des caractéristiques de quelques-uns des principaux logiciels clients EAP utilisés aujourd'hui dans le cadre du WiFi. Cette liste est bien sûr susceptible d'évoluer rapidement et est présentée à titre indicatif.

Logiciel client	Système d'exploitation	Principales méthodes EAP gérées
Xsupplicant (Open Source)	Linux	MD5, TLS, PEAP, TTLS, LEAP, SIM, GTC...
Client Windows	Windows XP	MD5, TLS, PEAP
Client Mac OS	Mac OS	MD5, TLS, PEAP, TTLS, LEAP
Odyssey	Windows et Pocket PC	MD5, TLS, PEAP, TTLS, LEAP
Aegis	Linux, Windows, Mac OS	MD5, TLS, PEAP, TTLS, LEAP

Le serveur d'authentification

Dans notre exemple, nous avons choisi un serveur de type RADIUS, car il s'agit de la solution presque universelle utilisée avec EAP. Toutefois, n'importe quel serveur compatible EAP peut faire l'affaire, comme par exemple un serveur Diameter. Le protocole Diameter a été défini en septembre 2003 dans la RFC 3588. Il s'agit d'une version améliorée du protocole RADIUS, mais il n'est pas encore très répandu.

> Lorsque l'on met en place une architecture 802.1x, le serveur d'authentification est généralement un serveur de type RADIUS.

Le choix du serveur est évidemment très important : comme pour le logiciel client, il faut évaluer attentivement son coût, les méthodes EAP qu'il gère, sa stabilité, les systèmes d'exploitation sur lesquels il peut être installé, son ouverture et le support fourni. Mais comme tout logiciel serveur, il faut également prendre en compte des facteurs tels que la performance, les outils de configuration disponibles, sa capacité à s'intégrer avec d'autres produits, notamment les bases de données, etc.

Voici les caractéristiques de quelques-uns des principaux serveurs RADIUS. Encore une fois, cette liste est susceptible d'évoluer et n'est ici qu'à titre indicatif. Nous présenterons le protocole RADIUS en détail au chapitre 10.

Serveur	Système d'exploitation	Principales méthodes EAP gérées
FreeRADIUS (Open Source)	Linux	MD5, TLS, PEAP, TTLS, LEAP, SIM
Microsoft IAS	Windows 2000 (inclus)	MD5, TLS, PEAP
Funk Software	Windows, Solaris, Netware, boîtier	MD5, TLS, PEAP, TTLS, LEAP, SIM
Radiator	Linux, Windows, Mac OS	MD5, TLS, PEAP, TTLS, LEAP, SIM
Meetinghouse	Windows, Linux, Solaris	MD5, TLS, PEAP, TTLS, LEAP, SIM
Infoblox	Boîtier	MD5, TLS, PEAP, TTLS, LEAP

Le contrôleur d'accès

Il y a bien peu de choses à dire au sujet du contrôleur d'accès, du point de vue de l'identification EAP : il ne sert que d'intermédiaire, et ouvre ou ferme la porte du réseau. En WiFi, il faut juste s'assurer que chaque AP gère le 802.1x et que celui-ci soit activé.

Toutefois, comme nous le verrons au § 8.2.3, les paquets EAP entre le contrôleur d'accès et le serveur d'authentification sont en général encapsulés dans des paquets RADIUS (si le serveur d'authentification est un serveur RADIUS bien sûr). Or ces paquets RADIUS peuvent transporter des paramètres très variés. Par exemple, le serveur peut informer le contrôleur d'accès qu'il ne faut laisser tel client se connecter que pendant 30 minutes, qu'il faut l'arrêter s'il reste inactif pendant 10 minutes ou dès qu'il aura téléchargé 2 Mo, que l'accès au sous-réseau 10.20.0.0/16 lui est interdit, et qu'il faut l'associer au VLAN numéro 30. Comme vous le voyez, ces paramètres RADIUS peuvent être très utiles pour gérer finement la connexion de chaque utilisateur. Toutefois, si l'on souhaite utiliser tous ces paramètres, il faut s'assurer qu'ils soient bien gérés par l'ensemble des contrôleurs d'accès (l'ensemble des AP). Ceci concerne cependant le protocole RADIUS, et nous y reviendrons donc au chapitre 10.

8.2.2 Les dialogues : quatre paquets

Types de paquets

EAP définit quatre types de paquets pouvant être échangés entre le client et le serveur d'authentification (par l'intermédiaire du contrôleur d'accès, bien sûr) :

- **Paquet Requête** : envoyé par le serveur d'authentification, il demande au client de fournir une information précise, comme son identité ou bien une preuve de cette identité, selon une méthode d'authentification choisie par le serveur (mot de passe, certificat électronique...).
- **Paquet Réponse** : envoyé par le client en réponse à une requête. Le contenu de la réponse dépend de la méthode d'authentification requise par le serveur. Si le client ne gère pas la méthode d'authentification requise, il le signale et en profite éventuellement pour suggérer une liste de méthodes qu'il est capable de gérer. Le serveur d'authentification peut alors choisir l'une de ces méthodes et renvoyer une nouvelle requête au client. Si aucune méthode ne lui convient, c'est un échec.
- **Paquet Succès** : envoyé par le serveur d'authentification pour indiquer au client qu'il a été correctement identifié. Au passage, le contrôleur d'accès ouvre la porte du réseau.
- **Paquet Échec** : envoyé par le serveur d'authentification, comme son nom l'indique, si le client n'a pas pu être identifié.

Voici le format d'un paquet EAP :

Code	ID	Longueur	Données
1 octet	1 octet	2 octets	*n* octets

Le champ « Code » indique s'il s'agit d'une requête, d'une réponse, d'un succès ou d'un échec. Le champ « ID » est un identifiant qui permet de savoir à quelle requête correspond une réponse. Le champ « Longueur » représente la longueur du paquet EAP. Dans les paquets de requêtes et de réponses, un champ « Type » (un octet) situé juste avant le champ de données indique quel type de méthode d'authentification est utilisée.

Exemple de dialogue EAP

Plusieurs séries de requêtes et réponses peuvent être échangées : en général le serveur d'authentification commence par demander au client son identité, puis il lui demande de s'identifier selon une méthode, ce qui entraîne parfois de nombreux échanges. Toutefois, dès que le client a commencé à répondre à une méthode d'authentification donnée, il ne peut plus revenir en arrière et choisir une autre méthode : il doit aller jusqu'au succès ou à l'échec de l'authentification. Ainsi, une seule méthode d'authentification peut être mise en œuvre au sein d'une même conversation EAP. Voici un exemple de conversation complète (voir aussi fig. 8.5) :

- le serveur d'authentification demande son identité au client ;
- le client répond, par exemple, « Patrice » ;
- le serveur d'authentification demande au client de s'authentifier avec une carte à jeton (voir § 8.3.4) ;
- le client ne gère pas les cartes à jeton, donc il refuse. Il en profite pour signaler qu'il sait s'authentifier avec un simple mot de passe ou avec un certificat électronique ;
- le serveur d'authentification préfère la méthode d'authentification par certificat électronique, donc il demande au client de s'authentifier de cette manière ;
- à ce moment, le client et le serveur d'authentification s'échangent plusieurs requêtes et réponses EAP contenant les informations nécessaires à l'authentification par certificat électronique ;
- une fois que le serveur d'authentification s'est assuré de l'identité du client, il envoie un paquet *Succès* au client. Ce paquet passe par le contrôleur d'accès qui laisse dorénavant le client accéder au réseau.

Dans la pratique, le client commence par signaler sa présence auprès du contrôleur d'accès, et celui-ci répond en général immédiatement en lui demandant son identité : cette première requête ne vient donc pas du serveur d'authentification. Par la suite, la conversation a bien lieu entre le client et le serveur d'authentification par le biais du contrôleur d'accès. C'est l'exception qui confirme la règle.

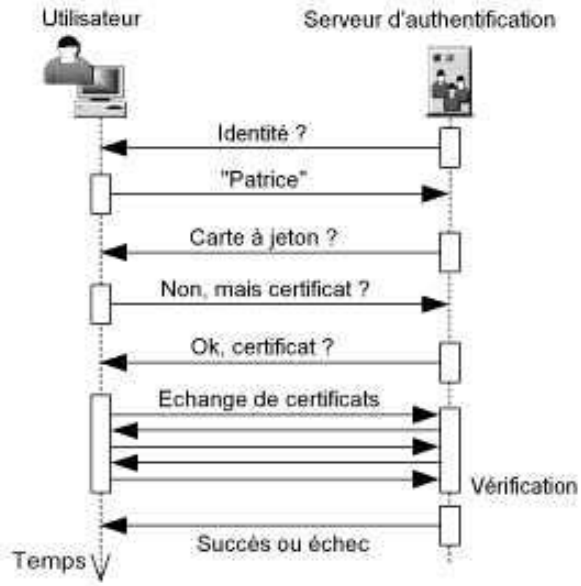


Figure 8.5 — Un exemple de dialogue EAP.

8.2.3 L'EAP et le 802.1x

Le protocole EAPoL

Le protocole EAP ne se soucie pas de savoir comment les paquets sont acheminés entre le client, le contrôleur d'accès et le serveur d'authentification, de sorte qu'il est possible d'utiliser EAP à l'intérieur d'un lien PPP, sur TCP/IP, UDP/IP, ou encore directement dans des paquets WiFi. La seule présupposition est qu'il existe un lien de communication entre le client et le contrôleur d'accès et un lien *sécurisé* (peu importe comment) entre le contrôleur d'accès et le serveur d'authentification.

Puisque dans le cadre du WiFi le contrôleur d'accès est un AP, le lien entre le client et l'AP est bien sûr un lien WiFi. Les paquets EAP sont donc encapsulés dans des paquets WiFi. Plus précisément, une version légèrement améliorée d'EAP est utilisée : *EAP over LAN* (EAP sur LAN), notée EAPoL. Ce protocole a été défini par le standard 802.1x pour permettre l'utilisation d'EAP dans un contexte où le client et le contrôleur d'accès communiquent *via* un réseau local (LAN). C'est bien le cas en WiFi. En outre, le 802.1x définit quelques nouveaux types de messages :

- **EAPoL-Start** : permet au client de prévenir le contrôleur d'accès qu'il souhaite se connecter ;
- **EAPoL-Packet** : ce sont ces paquets qui encapsulent les paquets EAP ;
- **EAPoL-Key** : permet l'échange de clés de cryptage ;
- **EAPoL-Logoff** : permet au client de demander la fermeture de sa session ;

- **EAPoL-Encapsulated-ASF-Alert** : permet aux clients dont l'authentification a échoué de pouvoir tout de même être supervisés à distance (par exemple, par SNMP). Ceci peut poser des problèmes de sécurité, donc le WPA et le WPA2 n'utilisent pas ce type de messages EAPoL.

Voici le format d'un paquet EAPoL :

En-tête MAC	Version	Type	Longueur	Message EAPoL
30 octets	1 octet	1 octet	2 octets	*n* octets

Le champ « Version » indique bien sûr la version du protocole EAPoL utilisé. Le champ « Type » indique s'il s'agit d'un paquet EAPoL-Start, EAPoL-Key, etc. Le champ « Longueur » indique la longueur du message qui suit.

Pour résumer : le 802.1x définit le protocole EAPoL qui permet de transporter les paquets EAP sur un LAN. Il définit en outre quelques autres types de paquets bien utiles. Nous verrons en particulier que les paquets EAPoL-Key sont essentiels pour le WPA Enterprise et le WPA2 Enterprise.

L'encapsulation RADIUS

La communication entre le contrôleur d'accès (c'est-à-dire l'AP) et le serveur d'authentification (le serveur RADIUS) se fait avec le protocole RADIUS. Les paquets EAP échangés entre le contrôleur d'accès et le serveur RADIUS sont donc encapsulés dans des requêtes RADIUS. La RFC 3579 détaille cette encapsulation (fig. 8.6).

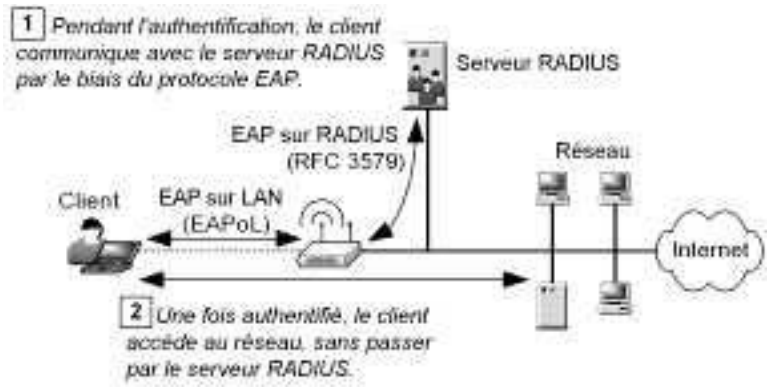


Figure 8.6 — Les protocoles du 802.1x.

Au chapitre 10, nous verrons que le protocole RADIUS permet de transporter des paramètres très variés. Les paquets EAP sont simplement transportés comme des paramètres normaux.

8.3 LES MÉTHODES EAP

En soit, l'EAP ne décrit que quelques méthodes d'identification, laissant à des RFC indépendantes (ou des *drafts*) le soin de définir une multitude d'autres méthodes. Voici un aperçu des principales méthodes d'identification actuellement utilisées.

8.3.1 EAP/MD5

Cette méthode d'authentification est définie dans la RFC 3748. Elle repose tout simplement sur le protocole CHAP étudié plus haut, avec le *hash* MD5.

8.3.2 EAP/MS-CHAP-v2

Cette méthode d'authentification EAP repose, comme son nom l'indique, sur le protocole MS-CHAP-v2. Il s'agit encore aujourd'hui d'un *draft*, mais il est déjà très utilisé, à commencer par Microsoft qui l'a inclus dans Windows.

Notons qu'il n'existe pas (encore) de méthode EAP/PAP ou EAP/MS-CHAP. Toutefois, nous verrons plus bas qu'il est possible d'utiliser PAP et MS-CHAP au sein de la méthode EAP/TTLS. D'autre part, EAP/GTC permet d'obtenir le même résultat que PAP, c'est-à-dire le transport d'un mot de passe, en clair.

8.3.3 EAP/OTP

Le système *One Time Password* (OTP) est défini dans la RFC 2289. L'utilisation des OTP avec EAP est définie dans la RFC 3748. Un OTP est un mot de passe conçu pour n'être utilisé qu'une seule fois. Ceci permet de l'échanger non crypté, sans craindre qu'il soit réutilisé par un pirate.

Voici comment cela fonctionne : le serveur commence par envoyer un défi au client. Ce défi contient quelques octets aléatoires et un index qui change à chaque nouveau défi. Le client doit alors utiliser un « générateur » (il s'agit en général d'un petit logiciel sur son ordinateur) afin de produire un OTP. Pour faire fonctionner le générateur, l'utilisateur doit lui fournir le défi (l'index et la séquence aléatoire) ainsi que son « vrai » mot de passe, appelé la « phrase secrète » ou *passphrase*. Le générateur fonctionne en faisant passer plusieurs fois (en fonction de l'index) le défi et la phrase secrète au travers d'une fonction de *hash*. Le résultat est un OTP de 8 octets que le client doit recopier et renvoyer au serveur. Recopier l'OTP manuellement est parfois source d'erreur, donc ces 8 octets sont parfois convertis (grâce à un simple tableau de correspondance) en une série de mots courts, moins difficiles à recopier, par exemple « OUST COAT FOAL MUG BEAK TOTE ». Le serveur peut effectuer les mêmes opérations et vérifier qu'il parvient bien au même résultat.

Le système OTP a été inventé et mis en œuvre par *Bell Communications Research* (Bellcore) dans leur produit S/Key. Il existe d'autres mises en œuvre, notamment un logiciel gratuit appelé OPIE (*OTP in Everything*, c'est-à-dire « OTP dans tout ») qui

s'installe facilement sur tout système Unix et sert à protéger l'accès au système et au service FTP avec le système OTP.

Malheureusement, comme le CHAP, le MS-CHAP et le MS-CHAP-v2, cette méthode est vulnérable aux attaques de dictionnaire hors-ligne : un pirate peut espionner une authentification réussie, puis essayer, chez lui, des milliers de mots de passe jusqu'à trouver celui qui aboutit au dialogue qu'il a espionné.

8.3.4 EAP/GTC

La RFC 3748 prévoit un type d'identification appelé *Generic Token Card* (carte à jeton générique). Cette méthode est très simple : le serveur envoie (optionnellement) un défi au client et celui-ci doit y répondre en tapant sa réponse, qui est renvoyée en clair. Le serveur vérifie la validité de la réponse et voilà !

Cette méthode très simple laisse une grande marge de manœuvre pour mettre en place des mécanismes très variés. En particulier, elle convient très bien (et a été conçue) pour les cartes à jeton. Ces cartes contiennent, comme leur nom l'indique, un « jeton » : un jeton est une clé assez longue qui n'est connue que par le serveur d'authentification et est nécessaire à l'identification du client. Ce dernier doit donc avoir sa carte avec lui lorsqu'il veut se connecter. Le plus souvent, un mot de passe est également exigé. On parle alors de sécurité à « double facteur » car, pour s'authentifier, l'utilisateur doit à la fois *connaître* quelque chose (son code PIN ou son mot de passe) et *posséder* quelque chose (la carte à jeton).

Les algorithmes sur lesquels reposent les cartes à jeton dépendent largement des constructeurs, mais la plupart utilisent le jeton, le mot de passe de l'utilisateur et le défi envoyé par le serveur pour générer un *hash* qui est renvoyé au serveur. Certaines cartes sont synchronisées avec le serveur et affichent un code qui change toutes les 10 à 20 secondes environ. Pour s'identifier, l'utilisateur doit taper ce code, ainsi que son mot de passe (ou code PIN).

Parmi les cartes à jeton les plus utilisées, on trouve par exemple les cartes SecurID (de RSA Security Inc.), les cartes d'Axent ou encore les Cryptocard. Certaines sont autonomes et possèdent un mini clavier voire même un petit écran à cristaux liquides. D'autres s'insèrent dans un lecteur de carte, connecté par exemple au port USB de l'ordinateur (fig. 8.7).

Figure 8.7 — Exemples de cartes à jeton.

Cette méthode d'authentification peut être la plus sûre qui soit, selon le type de carte à jeton que l'on utilise. Le jeton rend en effet impossibles les attaques de dictionnaire.

8.3.5 EAP/SIM

Cette méthode d'authentification est définie dans la RFC 4186. Son but est de permettre à un utilisateur de s'identifier grâce la carte SIM[1] de son téléphone portable GSM. Celle-ci peut être connectée à l'ordinateur *via* une clé USB, par exemple, ou directement intégrée dans l'adaptateur WiFi. Pour que l'identification puisse fonctionner, le serveur d'authentification doit être relié à l'opérateur mobile de l'utilisateur : il ne sert alors que d'intermédiaire entre le client et le serveur d'authentification de l'opérateur mobile. Cette solution a sans doute peu d'intérêt pour la plupart des entreprises dans le contexte d'un réseau WiFi (à part pour les opérateurs mobiles qui déploient des *hotspots*), mais il s'agit encore d'une nouvelle preuve de la convergence entre la téléphonie et les technologies de l'information. Par ailleurs, d'autres *drafts* ou RFC ont été écrits pour des méthodes d'identification liées à la téléphonie : EAP/SIM6 pour l'identification SIM passant par un réseau IPv6 et EAP/AKA pour l'identification par un réseau UMTS.

8.3.6 EAP/TLS

Un rappel sur TLS

Le protocole *Transport Layer Security* (TLS), nouvelle version de SSL, est défini dans la RFC 2246. Il est conçu pour établir un tunnel sécurisé entre un client et un serveur[2].

La mise en place d'un tunnel TLS commence par une première phase appelée la « négociation » ou « poignée de main » (*handshake*) : le serveur envoie son certificat électronique au client, et celui-ci fait de même, s'il en possède un. Le client est donc en mesure de s'assurer de l'identité du serveur, et *vice versa* si le client a envoyé son certificat.

À ce moment, le client génère une clé de cryptage symétrique. Il utilise ensuite la clé publique contenue dans le certificat du serveur pour crypter un message contenant la clé symétrique. Il l'envoie au serveur, qui est le seul à pouvoir décrypter le message et obtenir la clé symétrique. En effet, lui seul possède la clé privée correspondant à son certificat.

À la fin de la négociation TLS, le client s'est assuré de l'identité du serveur (et éventuellement *vice versa*), et une clé de cryptage symétrique a été secrètement échangée. Par la suite, les données échangées entre le client et le serveur sont cryptées grâce à cette clé symétrique.

---

1. *Subscriber Identity Module* : il s'agit de la carte à puce qui se trouve dans votre téléphone portable et qui sert entre autres à vous authentifier auprès de votre opérateur mobile.
2. Pour plus de détails sur le protocole TLS, les certificats et le cryptage asymétrique, voir l'annexe C sur le site *www.livrewifi.com*.

Bref, tous ces mécanismes confèrent à TLS un niveau de sécurité très important, tout en lui permettant de rester performant car seule la phase de négociation utilise le cryptage par clés asymétriques. TLS prévoit même un mécanisme optionnel pour compresser les données échangées dans le tunnel !

TLS dans EAP

Le protocole TLS est très complet, mais EAP ne se soucie que d'identification, pas de tunnel ou de compression de données. Par conséquent, EAP/TLS, qui est défini dans la RFC 2716, ne repose que sur la première phase de TLS : l'identification par certificat.

Pour utiliser EAP/TLS, il faut commencer par créer et installer un certificat électronique (et sa clé privée correspondante) sur le serveur d'authentification, ainsi que des certificats (et clés privées) distincts sur le poste de chaque utilisateur[1]. Lors du dialogue EAP, le client et le serveur s'échangent et vérifient leurs certificats en suivant le protocole TLS (fig. 8.8). L'authentification est très sûre et elle est mutuelle : ce sont les deux atouts majeurs d'EAP/TLS. En revanche, il y a plusieurs problèmes.

D'une part, le déploiement est assez lourd à gérer : créer, installer et maintenir des certificats électroniques différents sur chaque poste d'une entreprise peut devenir un véritable cauchemar. En outre, il peut arriver qu'une clé privée soit compromise : cela peut arriver si un ordinateur est volé, si un employé quitte la société (car il peut avoir conservé une copie de sa clé privée), ou encore si un pirate parvient à prendre le contrôle d'un ordinateur, car il peut alors trouver la clé privée et en faire une copie. Pour cette raison, les clés privées sont le plus souvent stockées dans des fichiers cryptés : seul l'utilisateur connaît le mot de passe permettant de décrypter sa clé privée et de l'utiliser. Quand une clé privée est compromise, il faut « révoquer » le certificat correspondant, c'est-à-dire le rajouter à la liste des certificats que le serveur doit rejeter.

> Le principal problème de l'authentification EAP/TLS est que chaque utilisateur doit posséder un certificat électronique : la gestion de ces certificats peut être assez lourde et poser des problèmes de sécurité.

Malgré ces lourdeurs, de plus en plus d'entreprises choisissent de mettre en place une Infrastructure à Gestion de Clé (IGC) ou *Public Key Infrastructure* (PKI). Des produits permettant de faciliter la création, le déploiement et la maintenance des certificats et des clés privées sont de plus en plus utilisés. En effet, les IGC permettent au mieux de sécuriser les systèmes en identifiant rigoureusement les utilisateurs et en leur permettant de crypter des documents ou de les signer électroniquement (ce qui permet de garantir la non-répudiation des transactions, dont nous avons parlé au chapitre 6, § 6.1.1).

1. En réalité, il n'est pas obligatoire d'installer un certificat sur le poste des clients, mais alors EAP/TLS permet juste aux clients de s'assurer de l'identité du serveur, pas l'inverse.

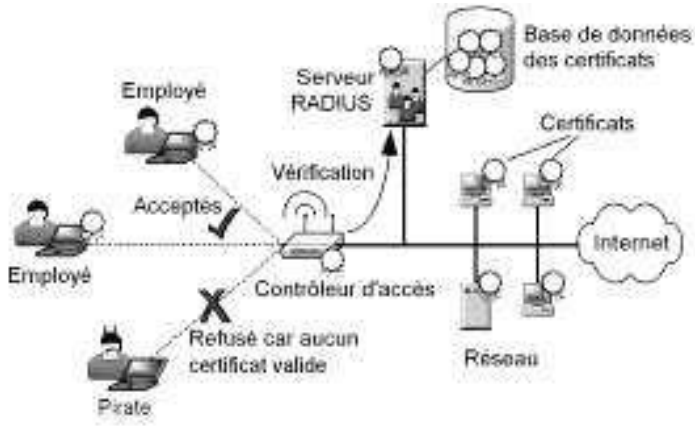


Figure 8.8 — L'authentification EAP/TLS.

Si EAP/TLS vous paraît trop lourd à gérer, mais que les méthodes précédentes vous paraissent peu sûres, alors les méthodes d'identification suivantes vous plairont sans doute davantage.

8.3.7 EAP/PEAP

Un EAP dans un tunnel

La méthode d'identification EAP/PEAP, en général appelée simplement « PEAP », a été développée par Cisco et Microsoft. « PEAP » signifie *Protected EAP*, c'est-à-dire « EAP Protégé ». Il s'agit encore pour le moment d'un *draft*, mais il devrait être promu au rang de RFC sous peu, vu son succès : PEAP est présent dans les dernières versions (mises à jour) de Windows.

Le principe de PEAP est le suivant : un tunnel TLS est d'abord mis en place entre le client et le serveur, puis une nouvelle négociation EAP (par exemple EAP/MS-CHAP-v2 ou EAP/GTC) se déroule au sein de ce tunnel, à l'abri des regards indiscrets. Voilà pourquoi l'on parle d'EAP « protégé ».

Voyons comment cela fonctionne (fig. 8.9). Au début, tout se passe à peu près comme pour EAP/TLS, mais avec quelques différences importantes :

- Au cours de la négociation EAP/PEAP, lorsque le serveur demande son identité au client, celui-ci n'est pas obligé de révéler sa véritable identité. Il peut répondre n'importe quoi (« anonyme », par exemple). Le serveur est parfois configuré pour ne même pas poser la question.
- Le client n'est pas obligé de fournir un certificat. Seul le serveur doit en fournir un pour prouver son identité au client.
- Plutôt que de s'arrêter à la fin de la négociation TLS (comme le fait EAP/TLS), EAP/PEAP va jusqu'à établir complètement le tunnel TLS.

- Dans ce tunnel, une nouvelle négociation EAP complète a lieu : c'est ici que le client fournit son identité et la preuve de cette identité. La méthode utilisée peut être n'importe quelle méthode EAP.
- Une fois que l'identification EAP « interne » est terminée par un paquet de succès ou d'échec, le tunnel TLS est fermé et le serveur renvoie un nouveau paquet de succès ou d'échec au client, en clair cette fois-ci. Sans cela, le contrôleur d'accès ne saurait pas s'il faut ou non laisser passer le client, car toute l'identification interne était cryptée.

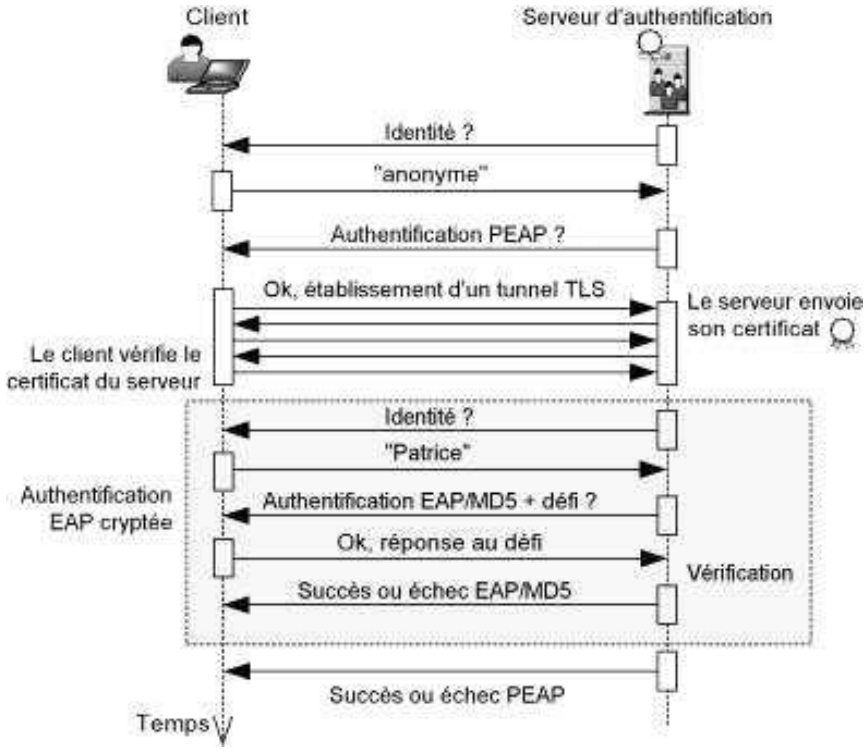


Figure 8.9 — L'authentification PEAP.

Puisque la méthode PEAP est toujours utilisée conjointement avec une autre méthode EAP, on précise toujours le nom de cette méthode interne, par exemple : PEAP/MD5 ou PEAP/OTP. Toutefois, aux yeux du contrôleur d'accès et de tout observateur extérieur, une seule méthode d'authentification est utilisée : EAP/PEAP.

Les avantages de PEAP

L'authentification qui a lieu à l'intérieur de PEAP est invisible au reste du monde. Ceci apporte deux avantages :

- la méthode d'identification interne est rendue plus sûre. On peut même envisager d'envoyer des mots de passe en clair ;

- l'identité même du client est cachée. Avec PEAP, un espion peut savoir que quelqu'un cherche à se connecter, mais il ne peut pas savoir qui.

> Puisque PEAP n'impose pas de déployer un certificat sur le poste de chaque client, il peut être assez simple à mettre en œuvre, tout en offrant un niveau de sécurité très important.

Toutefois, si on l'utilise avec une méthode interne qui repose sur un mot de passe, on est vulnérable à des attaques de dictionnaires (mais pas hors-ligne) : le pirate peut chercher à se connecter en essayant de nombreux mots de passe jusqu'à trouver le bon. Cependant, à moins qu'un utilisateur ait un mot de passe vraiment trivial, le pirate devra sans doute essayer plusieurs milliers de possibilités avant de trouver un mot de passe correct.

Il est donc recommandé de configurer le serveur pour qu'il bloque le pirate et alerte un administrateur dès qu'il détecte qu'une attaque de dictionnaire est en cours. Le fait que les attaques de dictionnaires ne soient possibles qu'en se connectant au système permet donc de réduire les exigences concernant la complexité des mots de passe. Ceci est une bonne chose pour la sécurité, car lorsqu'on demande à un employé de retenir un mot de passe très complexe et de le changer souvent, il a tendance à l'écrire quelque part, ce qui est pire que d'avoir un mot de passe modérément complexe ! Bien entendu, il faut tout de même proscrire les mots de passe les plus évidents comme « password », « /1234 » ou « azerty ».

8.3.8 EAP/TTLS

Une autre méthode de protection EAP assez populaire est l'EAP/TTLS, qu'on appelle en général simplement TTLS (*Tunneled TLS*). Comme PEAP, la méthode TTLS est encore un *draft*. Comme PEAP, TTLS commence par établir un tunnel TLS, puis met en œuvre une autre authentification dans ce tunnel. Les points communs avec PEAP sont en fait si nombreux qu'il est plus rapide de parler de leurs différences :

- TTLS a été conçu par la société Funk Software, connue par ailleurs pour son serveur RADIUS : *Steel-Belted RADIUS* et sa solution de sécurité pour réseaux WiFi : *Odyssey* ;
- TTLS n'est pas intégré dans Windows ;
- TTLS autorise tout type d'identification interne et pas uniquement EAP. Par exemple, on peut utiliser directement PAP (l'envoi d'un mot de passe en clair) dans TTLS, ou encore CHAP, MS-CHAP ou MS-CHAP-v2 ;
- il est possible de rajouter des paires d'attribut/valeur (*Attribute-Value Pair*, AVP) dans les paquets TTLS.

Une AVP est composée du type de l'attribut et de sa valeur. Par exemple : [Prénom, « Emmanuelle »]. Une AVP est généralement transmise selon le format suivant : un numéro qui indique le type, suivi d'un nombre qui précise la longueur totale de l'AVP

(incluant le type et la longueur), suivi enfin de la valeur du champ. On parle donc de champ Type/Longueur/Valeur (TLV), qui transporte une AVP.

La possibilité pour le client et le serveur de s'échanger des AVP est intéressante, car ceux-ci peuvent transporter des informations supplémentaires, outre les informations liées à l'authentification. Ceci peut être utile de multiples façons : en particulier, il est possible d'envoyer des paramètres de configuration au poste du client. Par exemple, on peut imaginer que certains AVP contiennent des règles pour le pare-feu du client et que le logiciel de connexion du client soit capable de les mettre en place automatiquement. On peut bien sûr imaginer toutes sortes d'autres applications. Le *draft* de TTLS, quant à lui, propose notamment que les AVP soient utilisées pour que le client et le serveur négocient des clés de cryptages : une fois le client identifié et autorisé à accéder au réseau, ces clés lui permettront de crypter toutes ses communications avec le contrôleur d'accès et sécuriser ainsi son accès au réseau. Cependant, le WPA Enterprise et le WPA2 Enterprise utilisent une autre solution, qui repose en partie sur les paquets EAPoL-Key.

L'autre avantage des AVP est que le protocole RADIUS repose également sur des AVP. Cela peut faciliter la configuration des serveurs RADIUS, si l'on souhaite renvoyer des AVP spécifiques à des clients au travers du protocole EAP/TTLS.

Il a été suggéré que le protocole EAP soit légèrement modifié pour autoriser l'échange d'AVP, mais ceci n'est pas encore d'actualité.

8.3.9 PEAP ou TTLS ?

Vu le peu de différences entre PEAP et TTLS, on est en droit de penser que l'un ou l'autre risque de disparaître, à plus ou moins brève échéance. Les arguments en faveur de PEAP sont les suivants : d'une part il est soutenu par deux des acteurs les plus puissants du marché, Microsoft et Cisco et d'autre part il est déjà intégré dans le poste de toute personne qui possède une version récente de Windows, contrairement à TTLS qui suppose l'installation d'un logiciel sur le poste du client.

De son côté, TTLS est légèrement plus flexible que PEAP, surtout grâce aux AVP qui permettent de transférer tout type d'information. En outre, certaines personnes apprécient le fait que TTLS permette aux clients d'envoyer leur mot de passe en clair, grâce à TTLS/PAP. Ce n'est pas le cas de PEAP, puisque PAP n'est pas une méthode EAP (ou pas encore), or seules les méthodes EAP sont autorisées avec PEAP.

Seul l'avenir dira si PEAP ou TTLS doit disparaître ! Si c'est le cas et que vous faites le mauvais choix aujourd'hui, il faudra revoir une partie de l'architecture de votre système de sécurité. Et si les deux survivent, il arrivera peut-être que vous ayez parfois à jongler entre les deux systèmes. Les temps sont durs...

8.3.10 EAP/FAST

EAP dans un tunnel symétrique

Il faut signaler une autre méthode d'authentification par tunnel, publiée en février 2004 par Cisco sous la forme d'un *draft* IETF : EAP/*Flexible Authentication via*

Secure Tunneling (EAP/FAST). Il est très similaire à TTLS : un tunnel est créé pour protéger une authentification interne et des TLV peuvent être échangés. Mais il y a une différence de taille : le tunnel peut être établi avec un algorithme de cryptage symétrique et non avec TLS. Ceci présente essentiellement deux intérêts :

- il n'est pas nécessaire d'installer un certificat sur le serveur ;
- la création du tunnel est plus rapide avec un algorithme symétrique qu'avec TLS (d'où le jeu de mot avec *fast* qui signifie « rapide »).

Avec EAP/TLS, PEAP et TTLS, il est nécessaire d'installer un certificat (et une clé privée) sur le serveur d'authentification. Cela ne prend pas, en soi, énormément de temps. Toutefois, le certificat doit être signé par une autorité de certification (*Certification Authority*, CA) connue de tous les utilisateurs. On a donc deux options : soit on génère un certificat et on le fait signer par une société tierce dont c'est le rôle, du type *Verisign* ou *Thawte*[1], ce qui peut prendre quelques semaines et coûter plusieurs centaines d'euros, soit on décide de signer soi-même le certificat du serveur en jouant le rôle d'autorité de certification. Pour cela, il faut générer un certificat de type CA et on l'utilise pour signer le certificat du serveur. Reste ensuite à déployer ce certificat CA sur les postes de tous les utilisateurs, ce qui peut être assez long.

Puisque EAP/FAST est capable de créer le tunnel d'authentification en utilisant un algorithme symétrique, il permet de se dispenser du certificat du serveur. Mais un nouveau problème se pose : pour établir un tunnel avec un algorithme symétrique, il faut que le serveur partage une clé avec chaque client ! Ces clés sont stockées dans des fichiers protégés par un mot de passe : les *Protected Access Credentials* (PAC)[2]. Pour mettre en place un système basé sur EAP/FAST, il faut donc commencer par utiliser un outil pour générer un PAC pour chaque utilisateur et installer le bon PAC sur le poste de chaque utilisateur. On se rend donc compte que ce système est tout aussi lourd à gérer que EAP/TLS ! Le *draft* d'EAP/FAST suggère toutefois des méthodes pour la distribution des PAC. Malheureusement, les méthodes les plus sûres impliquent un mécanisme à base de certificats : on tourne donc en rond. Contrairement aux annonces marketing, l'EAP/FAST n'est donc pas réellement plus facile à administrer que EAP/TLS et certainement nettement plus difficile que TTLS ou PEAP.

Une authentification rapide

Le seul véritable avantage de EAP/FAST est donc le second : l'authentification est plus rapide. Mais attention : la différence n'est en général pas sensible pour un utilisateur, car quelle que soit la méthode choisie, tout se passe en une fraction de seconde. Le seul scénario où l'utilisateur peut éventuellement voir une différence, dans le contexte du WiFi, est le changement de cellule : lorsqu'un utilisateur déjà associé et authentifié se déplace avec son ordinateur et arrive à proximité d'un autre AP du même réseau sans fil, son ordinateur le détecte et change automatiquement d'AP (fig. 8.10).

1. Les certificats de ces sociétés sont déjà présents sur les postes de tous les utilisateurs, car ils sont installés en même temps que le système d'exploitation.
2. Littéralement, cela signifie « preuve d'identité à accès protégé ».

Malheureusement, l'utilisateur doit alors se réauthentifier auprès de ce nouvel AP ! Pour cette raison, le logiciel EAP de l'utilisateur, s'il est malin, conserve toutes les informations nécessaires pour le réauthentifier automatiquement. Toutefois cela peut prendre quelques précieuses fractions de seconde. La plupart du temps, l'utilisateur ne se rendra compte de rien, mais s'il est en conversation téléphonique en voix sur IP, par exemple, il entendra peut-être une brève coupure. La rapidité de l'EAP/FAST permet donc de réduire ce délai de *handover*. Notons que l'IEEE a publié un amendement à la norme 802.11, le 802.11r, qui permet au *handover* de se déplacer plus rapidement.

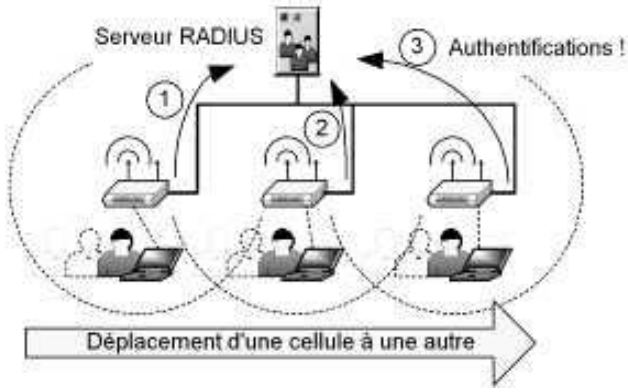


Figure 8.10

Bref, si la lourdeur administrative de EAP/FAST ne vous fait pas peur, qu'il est important à vos yeux que le délai de *hand-over* d'une cellule à une autre soit très faible, alors EAP/FAST peut vous convenir. Toutefois, le protocole EAP/FAST n'est encore guère promu que par Cisco.

8.3.11 Autres méthodes EAP

La liste, déjà longue, des méthodes EAP est susceptible de s'allonger encore considérablement au cours des années à venir, d'autant que l'engouement pour l'EAP semble s'amplifier de jour en jour depuis qu'il est à la base des nouvelles solutions de sécurité du WiFi. Parmi les méthodes qui voient le jour, certaines ne survivent pas longtemps ou stagnent sans que des produits ne les mettent en œuvre.

C'est le cas semble-t-il de EAP/GSS, dont le *draft* a expiré sans passer au rang de RFC. Ce *draft* a de nouveau été proposé et il est possible qu'il parvienne un jour à devenir une RFC, mais il est impossible d'en être sûr aujourd'hui. Ce *draft* définit une méthode EAP reposant sur le système de sécurité Kerberos, au travers de l'interface de programmation *Generic Security Service* (GSS) qui est conçue pour permettre l'interconnexion avec ce système de sécurité. Pour plus d'information sur le système Kerberos, consultez le site web de l'Institut de Technologie du Massachusetts (*www.mit.edu*).

8.4 LA SÉCURITÉ D'EAP

8.4.1 Les failles

Le protocole EAP possède quelques failles bien identifiées. En faisant attention, il est heureusement possible de toutes les éviter, comme nous allons le voir. Voici les trois failles principales, que nous allons détailler :

- un pirate peut essayer d'attaquer la méthode d'authentification EAP choisie (EAP/MD5 par exemple) elle a ses propres failles ;
- un pirate peut attendre que la session soit établie et ensuite attaquer cette session : en effet, le protocole EAP ne dit rien sur la façon de protéger la connexion au réseau, une fois qu'elle est établie ;
- un pirate peut s'intercaler entre le client et le contrôleur d'accès (attaque de type MiM) et être ainsi authentifié à la place du client.

8.4.2 L'attaque de la méthode EAP

L'attaque contre la méthode d'authentification est bien sûr la plus évidente à concevoir : si la méthode d'authentification n'est pas sûre, naturellement, un pirate peut s'y attaquer. Nous avons déjà abordé quelques-unes de ces attaques, mais nous allons les résumer ici.

Attaques de dictionnaire hors-ligne

Prenons EAP/MD5, par exemple : son mécanisme est bien connu, il est utilisé depuis très longtemps et il semble assez fiable au premier abord. Rappelons le principe : le serveur envoie un défi nouveau à chaque authentification, le client utilise l'algorithme MD5 pour calculer un *hash* à partir de ce défi et il le renvoie au serveur. Celui-ci peut alors faire le même calcul et s'assurer qu'il obtient bien le même résultat.

Le problème est le suivant : si un pirate peut espionner une identification complète, il obtiendra le défi et le *hash* correspondant. Il peut alors lui-même calculer un *hash* à partir du défi et d'un mot de passe de son choix. S'il obtient le bon *hash*, il sait qu'il a trouvé le bon mot de passe. Sinon il lui suffit de recommencer, encore et encore. Puisqu'il peut faire ceci dans son coin, sans avoir à se connecter au réseau (c'est-à-dire « hors-ligne »), il n'a aucun risque d'être repéré. Il lui suffit de lancer un programme sur son ordinateur, qui vérifie des millions de mots de passe probables : c'est une attaque de type « dictionnaire ». Bien sûr, une fois qu'il a trouvé le bon mot de passe, il n'a plus qu'à se connecter comme un utilisateur normal ! Et s'il ne parvient pas à trouver le mot de passe d'un utilisateur donné, il lui suffit de passer au suivant : il y en a bien un qui aura un mot de passe assez simple.

La seule façon de lutter efficacement contre cette attaque est de s'assurer que tous les utilisateurs possèdent un mot de passe complexe. Or, presque aucune société ne peut affirmer que ses employés utilisent tous des mots de passe complexes. Certaines sociétés tentent bien d'imposer à leurs employés qu'ils changent de mot de passe toutes les deux semaines, qu'ils ne réutilisent jamais un ancien mot de passe, qu'ils n'utilisent

qu'une succession aléatoire de lettres en majuscules ou non, de chiffres ou de symboles. Malheureusement, les employés oublient leur mot de passe ou bien le collent sur leur écran avec un « post-it » : la sécurité n'est pas forcément améliorée ! Bref, EAP/MD5 ne doit pas être utilisé s'il y a un risque que la communication soit écoutée : or, en WiFi, un pirate peut écouter toutes les communications, sans difficulté. Conclusion : pas de EAP/MD5 en WiFi ?

Attaques de dictionnaire en ligne

Heureusement, il y a les tunnels : avec PEAP, TTLS et EAP/FAST, la méthode d'authentification interne est protégée. Si l'on utilise PEAP/MD5, par exemple, on n'a pas à craindre d'attaque de dictionnaire hors-ligne. Si un pirate veut essayer des milliers de mots de passe, il devra les soumettre au serveur d'authentification. Pour avoir un bon niveau de sécurité avec PEAP/MD5, il faut donc :

- mettre en place un système qui évite qu'un pirate puisse essayer des milliers de mots de passe d'affilée : par exemple, on peut configurer le serveur d'authentification pour qu'il refuse toute nouvelle tentative de connexion d'un même utilisateur après trois tentatives infructueuses et ce pendant 5 minutes ;
- vérifier régulièrement les historiques (les « *logs* ») de connexion, afin de détecter les tentatives d'intrusion. Il existe des analyseurs de *logs* destinés à cet effet. Ils peuvent analyser les *logs* en permanence et prévenir l'administrateur en cas d'attaque ;
- demander aux employés d'avoir un mot de passe raisonnablement complexe : il n'est plus nécessaire qu'il soit long et extravagant (ce qui va soulager tout le monde), mais au moins il faut qu'un pirate ne puisse pas le trouver en quelques milliers de tentatives. Il faut donc toujours éviter des mots de passe trop simples, comme « admin » ou « david », mais on peut se permettre un mot de passe comme « W1fiSek » qui serait beaucoup trop faible face à une attaque de dictionnaire hors-ligne.

Les méthodes EAP/MS-CHAP-v2 et EAP/OTP sont également vulnérables aux attaques de dictionnaire hors-ligne : on ne doit donc les utiliser qu'au sein d'un tunnel.

Pour EAP/GTC et EAP/SIM, l'authentification elle-même est assez sûre. Malheureusement, nous verrons que ces méthodes sont vulnérables aux deux autres attaques, de sorte qu'on conseille vivement de les utiliser également au sein d'un tunnel, dans le cadre du WiFi.

> Pour atteindre le meilleur niveau de sécurité, il est recommandé d'utiliser les tunnels : EAP/TLS, PEAP, TTLS ou EAP/FAST.

8.4.3 L'attaque de la session

EAP seul ne protège pas la session

Imaginons qu'un utilisateur s'associe à un AP et s'identifie en utilisant la méthode EAP/TLS. Imaginons également qu'aucune autre mesure de sécurité ne soit mise en

place au niveau du réseau sans fil. La méthode d'authentification choisie est l'une des plus sûres, donc un pirate aura beaucoup de mal à s'y attaquer. Toutefois, voyons ce qui se passe une fois que l'utilisateur est authentifié avec succès : l'AP accepte dorénavant tous les paquets en provenance de l'adresse MAC de cet utilisateur. En outre, le travail de EAP étant terminé, le tunnel TLS est fermé : cela signifie que tous les paquets du client sont maintenant échangés en clair.

C'est la catastrophe ! Non seulement un pirate peut écouter toutes les communications du client, en clair, mais il lui suffit de configurer son adaptateur WiFi et de lui donner la même adresse MAC que le client pour pouvoir détourner ainsi sa session et accéder au réseau : on appelle cela le « *spoofing* d'adresse MAC » (voir le § 6.2.3 du chapitre 6). On se demande bien pourquoi l'on a mis tant d'efforts à sécuriser l'authentification si la session créée peut être détournée aussi aisément ? On voit, dans cet exemple, qu'il y a en réalité deux identifications : la première est réalisée par le serveur d'authentification avec EAP ; la seconde est réalisée ensuite par le contrôleur d'accès, sans l'aide d'EAP, à chaque paquet envoyé par le client. Or, le contrôleur d'accès identifie le client comme il le peut, c'est-à-dire avec son adresse MAC, ce qui n'offre qu'une protection très limitée.

> **Résumons** : l'EAP, sans l'aide d'autres mécanismes, ne protège que l'authentification, pas la session. Donc si l'on ne fait rien de plus qu'EAP (c'est-à-dire du 802.1x seul) alors un pirate peut espionner ou détourner les sessions existantes, en toute impunité. Mais alors, comment se protéger ?

Un tunnel entre le client et le contrôleur d'accès

Clé statique ou négociation dynamique

La meilleure solution pour protéger la session consiste à mettre en place un tunnel entre le client et le contrôleur d'accès. De cette façon, un pirate ne pourra ni espionner ni détourner la session. Pour bien protéger la session, ce tunnel doit mettre en œuvre un cryptage puissant et empêcher toute attaque de relecture.

Pour que le client et le contrôleur d'accès puissent crypter leurs échanges, il est nécessaire qu'ils utilisent une même clé de cryptage[1]. On a deux options :

- la clé peut être configurée manuellement dans le logiciel client et le contrôleur d'accès ;
- la clé peut être négociée automatiquement au cours de l'authentification.

La première option est très simple et elle est possible avec le WPA Personal et le WPA2 Personal, comme nous le verrons au prochain chapitre. Pour comprendre la deuxième option, revenons un instant sur la méthode d'authentification EAP/TLS. Nous avons vu qu'au cours de la négociation TLS, le client génère une clé, puis la crypte en utilisant la clé publique du serveur et lui envoie. De cette façon, le client et le serveur parviennent à s'échanger une clé tout à fait secrètement. On dit que

1. Nous verrons au chapitre 9 que plusieurs clés de cryptage sont en réalité nécessaires, mais qu'elles peuvent être dérivées d'une première clé « maîtresse » : la *Primary* Master *Key* (PMK).

la méthode EAP/TLS est « génératrice de clé ». Il suffit alors au serveur d'envoyer (secrètement) cette clé à l'AP, par le biais d'un paquet RADIUS prévu à cet effet. De cette façon, le client et l'AP possèdent la même clé et peuvent établir un tunnel sécurisé ! Nous détaillerons ce mécanisme au prochain chapitre, c'est le principe d'échange de clé sur lequel reposent le WPA Enterprise et le WPA2 Enterprise.

> L'authentification 802.1x peut être très sûre, mais elle ne sert à rien si la session qui suit n'est pas elle-même sécurisée. La session peut être protégée par un tunnel entre le client et le contrôleur d'accès. Celui-ci peut être mis en place au cours de l'authentification 802.1x.

Un mot sur LEAP

Au sujet du changement dynamique de clé de cryptage, il faut mentionner la solution *Lightweight EAP* (LEAP), c'est-à-dire « l'EAP Léger », développée par Cisco. Il s'agit de la première solution de sécurité WiFi à avoir exploité le 802.1x. Ce protocole repose sur une méthode d'authentification propriétaire, basée sur un mot de passe. Lors de l'authentification, une clé WEP est mise en place automatiquement entre le client et l'AP, par le biais d'un algorithme propriétaire : ceci simplifie grandement la gestion du réseau, par rapport à la solution WEP classique. Pendant la session du client, l'AP peut régulièrement changer la clé WEP, en fournissant la nouvelle clé au client. Ceci rend naturellement le cryptage beaucoup plus sûr.

Cette solution a été la plus puissante pendant assez longtemps, mais depuis l'arrivée du WPA, elle est peu recommandée car elle repose sur le cryptage WEP, dont nous avons étudié les faiblesses. En outre, seule l'authentification par mot de passe est possible alors que le WPA est bien plus souple.

8.4.4 Les attaques MiM

Une attaque simple à réaliser

Comme nous l'avons vu, EAP a été conçu à l'origine pour PPP. Dans ce contexte, il est raisonnable de penser qu'on est relativement à l'abri d'une attaque de type MiM : en effet, si un utilisateur se connecte à Internet par le biais d'un modem téléphonique, il est difficile pour un pirate de s'interposer entre le poste de cet utilisateur et le PoP. Il faudrait que le pirate puisse prendre le contrôle de la communication téléphonique, ce qui n'est pas à la portée du premier venu. Il y aurait d'autres méthodes, mais d'une façon générale, elles sont toutes assez difficiles à réaliser.

Malheureusement, dans le contexte du WiFi, il est assez facile pour un pirate de s'insérer entre le client et le contrôleur d'accès (c'est-à-dire l'AP). Nous avons vu au chapitre précédent (§ 7.3.2) qu'il lui suffisait d'installer un AP pirate configuré avec le même SSID que les AP légitimes. Une fois qu'un client est associé à cet AP pirate, le pirate n'a plus qu'à s'associer à un AP légitime et à servir d'intermédiaire entre le client et l'AP légitime. Autant le client que l'AP légitime auront l'impression de parler directement l'un avec l'autre, mais au final ce sera le pirate qui sera autorisé à rentrer sur le réseau !

Pour vous en convaincre, revenons à notre histoire de gardien. Cette attaque fonctionne ainsi : le pirate commence par se déguiser en gardien. Un client souhaitant rentrer sur le réseau s'adresse à lui et lui fournit son nom. Le pirate va alors s'adresser au véritable gardien. Il lui répète le nom du client. Le gardien va lui-même le répéter au patron puis revient avec, par exemple, un défi. Le pirate remet alors son déguisement de gardien et répète le défi au client. Lorsque le client donne sa réponse, le pirate n'a plus qu'à aller la répéter au gardien. Après vérification auprès du patron, le gardien laisse alors rentrer le pirate. L'attaque a réussi (fig. 8.11).

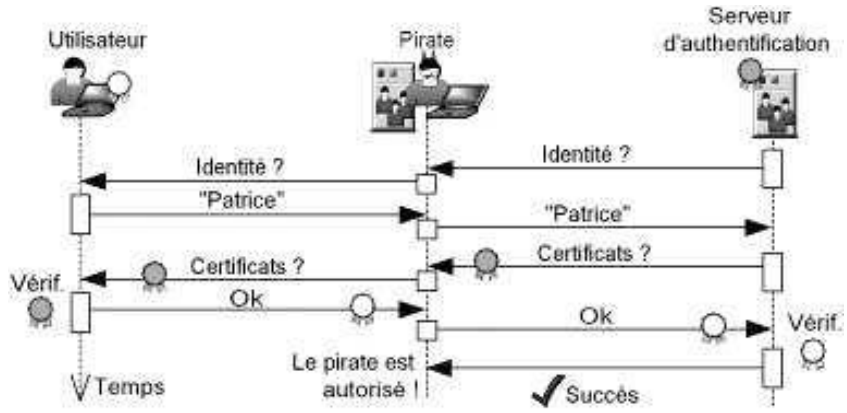


Figure 8.11 — Attaque MiM contre l'authentification EAP.

Dans cette histoire, on voit que le pirate n'a aucunement besoin de comprendre quoi que ce soit au contenu des paquets EAP qu'il transporte. Notons que EAP/TLS, PEAP, TTLS ou EAP/FAST sont tout aussi vulnérables que les autres méthodes : en se plaçant entre le client et le contrôleur d'accès et en répétant tout se qui se dit, le pirate fini par se faire accepter.

La parade : le cryptage de la session

La seule parade contre cette attaque MiM consiste à mettre en place un cryptage puissant pour la session. Les clés de cryptage peuvent être configurées manuellement ou échangées au cours de l'authentification, comme nous l'avons vu plus haut. De cette façon, même si le pirate parvient à se faire accepter sur le réseau, il ne pourra ni envoyer ni recevoir de paquets, car il ne connaîtra pas les clés de cryptage.

Attaque contre PEAP et TTLS

Les méthodes PEAP et TTLS ont une vulnérabilité supplémentaire, qu'il est heureusement facile d'éviter : le pirate peut essayer de créer un tunnel avec le client et un tunnel avec le serveur. Il peut alors avoir accès à la méthode d'authentification « interne » utilisée, qui est souvent très vulnérable. Voici comment il peut procéder (fig. 8.12) :

- le pirate configure sont poste pour se comporter comme un AP (même SSID qu'un AP légitime) ;

- lorsqu'un client cherche à se connecter à lui avec la méthode PEAP ou TTLS, le pirate ne redirige pas encore les paquets à un AP légitime. Au contraire, il se comporte comme le serveur d'authentification et envoie un faux certificat au client pour établir un tunnel sécurisé ;
- si le client ne vérifie pas rigoureusement le certificat qui lui est envoyé, il peut croire avoir affaire au serveur d'authentification légitime. Il utilise alors le tunnel créé entre lui et le pirate pour négocier la méthode EAP interne ;
- à ce moment, le pirate négocie lui-même un tunnel PEAP ou TTLS avec le serveur d'authentification, via un AP légitime. Au sein de ce tunnel, il redirige tout le trafic EAP interne et fini par accéder au réseau.

À l'issue de cette attaque, non seulement le pirate est accepté complètement sur le réseau, avec ses propres clés de cryptage, mais en plus il a vu passer la négociation EAP interne en clair. Or cette négociation interne est généralement très simple et vulnérable : par exemple, avec PAP, le mot de passe est envoyé en clair à l'intérieur du tunnel, avec EAP/MD5, le pirate peut faire une attaque de dictionnaire hors-ligne, etc.

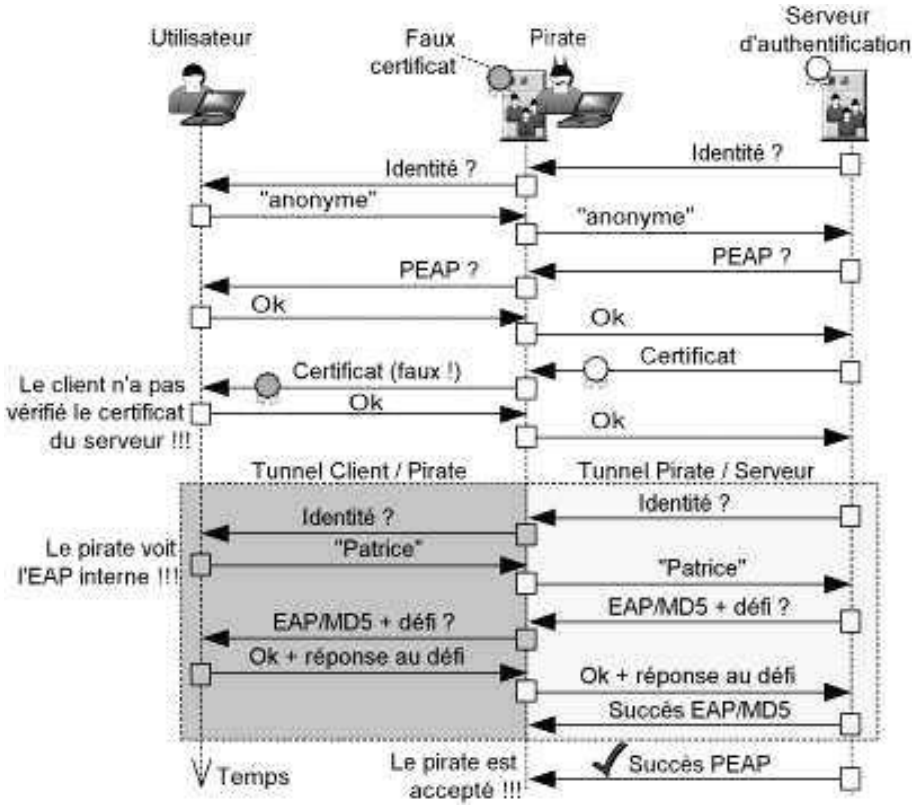


Figure 8.12 — Attaque MiM contre les authentifications reposant sur TLS.

Comment éviter cette terrible attaque ? La première solution est simple : il suffit de s'assurer que tous les clients vérifient bien le certificat envoyé par le serveur. De cette façon, ils refuseront le faux certificat envoyé par le pirate. La vérification du certificat est généralement réalisée automatiquement par le logiciel de connexion 802.1x : si le certificat est mauvais, le logiciel affiche en général un message d'avertissement à l'utilisateur. Informez à tout prix les utilisateurs que ces messages d'avertissement sont à prendre très au sérieux et qu'il faut refuser toute connexion et prévenir l'administrateur lorsqu'un tel message s'affiche. Certains logiciels peuvent être configurés pour interdire toute connexion si le certificat du serveur est mauvais : il faut activer cette option !

> Lorsqu'on utilise EAP/TLS, PEAP ou TTLS, il faut à tout prix s'assurer que le certificat du serveur soit bien vérifié par les clients : sans cela, un pirate peut facilement prendre le contrôle total d'une session.

Une deuxième solution consiste à mettre en place un certificat sur le poste de chaque utilisateur et à configurer le serveur d'authentification pour qu'il vérifie bien la validité du certificat. Dans ce cas, on perd l'un des avantages de PEAP et TTLS qui était d'éviter la lourdeur administrative de EAP/TLS. Cependant, cela empêchera le pirate de créer un tunnel avec le serveur d'authentification.

8.4.5 Une bonne sécurité avec le 802.1x

Pour bénéficier de la meilleure sécurité possible avec le 802.1x et éviter ses quelques failles, il faut donc :

- utiliser une des méthodes à base de tunnel : EAP/TLS, TTLS ou PEAP (voire EAP/FAST) ;
- s'assurer que le certificat du serveur soit *toujours* vérifié par les clients et qu'aucun utilisateur ne se connecte si le certificat est mauvais ;
- éventuellement mettre en place un certificat pour chaque poste client ;
- utiliser si possible une méthode interne assez forte, telle qu'une carte à jeton ;
- s'assurer qu'un cryptage puissant soit mis en place au cours de l'identification : le WPA et le WPA2 sont d'excellentes options.

Résumé

Le protocole 802.1x, défini par l'IEEE, repose sur le protocole EAP. Ce dernier, défini par l'IETF, a pour rôle d'identifier les utilisateurs selon des méthodes variées : mot de passe, carte à jeton, certificat, etc. L'EAP définit une architecture comptant trois acteurs : le *client* (c'est-à-dire l'utilisateur), le *contrôleur d'accès* (c'est-à-dire chaque point d'accès, dans le contexte du WiFi) et le *serveur d'authentification* (en général un serveur RADIUS). Le client commence par se connecter au contrôleur d'accès. Celui-ci l'empêche d'aller sur le réseau. Commence alors un dialogue d'authentification entre le client et le serveur d'authentification, par l'intermédiaire du contrôleur

d'accès. Si le serveur autorise le client à passer, il lui envoie un paquet EAP de succès : au passage de ce paquet, le contrôleur d'accès laisse désormais le client accéder au réseau.

Le protocole 802.1x définit comment le protocole EAP peut être utilisé sur un réseau local, grâce au protocole EAPoL. Ce dernier rajoute notamment quelques nouveaux paquets permettant l'échange de clés de cryptage.

Pour mettre en place une architecture 802.1x avec le WiFi, il faut choisir et installer un serveur d'authentification (en général de type RADIUS), et s'assurer que tous les AP gèrent bien le 802.1x. Il faut également choisir et installer un logiciel de connexion compatible 802.1x sur le poste de chaque utilisateur. Ce logiciel peut être fourni avec l'adaptateur WiFi ou directement intégré dans le système d'exploitation : c'est le cas avec les versions récentes de Windows et de Mac OS. Il reste ensuite à choisir une ou plusieurs méthodes d'authentification EAP, s'assurer que le serveur RADIUS les gère et que les logiciels de connexion des clients soient bien compatibles avec au moins l'une de ces méthodes.

Les principales méthodes d'authentification EAP sont EAP/MD5 (mot de passe), EAP/MS-CHAP-v2 (mot de passe), EAP/OTC (mot de passe), EAP/GTC (carte à jeton), EAP/SIM (carte SIM) et EAP/TLS (certificat électronique). Par ailleurs, trois autres méthodes EAP ont pour but de protéger une authentification EAP au sein d'un tunnel sécurisé : EAP/PEAP, EAP/TTLS et EAP/FAST.

La sécurité du 802.1x peut être compromise de trois façons différentes : en attaquant la méthode EAP utilisée, en détournant une session après sa création ou encore en s'interposant entre le client et le serveur d'authentification. Pour éviter toutes ces attaques, nous avons vu qu'il fallait :

– utiliser une méthode d'authentification basée sur un tunnel : EAP/TLS, TTLS ou PEAP (voire EAP/FAST) ;

– s'assurer que les clients ne se connectent que si le certificat envoyé par le serveur est valide ;

– éventuellement, utiliser un certificat par poste client et le faire vérifier par le serveur (c'est malheureusement plutôt lourd à gérer) ;

– utiliser une méthode interne assez forte, comme les cartes à jeton par exemple ;

– s'assurer qu'un cryptage puissant soit négocié pendant l'identification : le WPA et le WPA2 sont les meilleures solutions pour le WiFi... et nous allons les étudier maintenant.

9

Le WPA et le WPA2

Objectif

Dans le chapitre précédent, nous avons vu que le 802.1x permet de mettre en place des méthodes d'authentification des utilisateurs très sûres et très variées : l'envoi d'un simple mot de passe au sein d'un tunnel TLS, l'utilisation d'une carte à jeton ou encore l'échange de certificats électroniques, le tout centralisé par un serveur d'authentification. En outre, le 802.1x permet l'échange de clés de cryptage qui peuvent servir à sécuriser les communications entre l'utilisateur et le contrôleur d'accès (c'est-à-dire l'AP auquel l'utilisateur est associé).

Dans ce chapitre, nous allons étudier les meilleures solutions de sécurité du WiFi, le WPA et le WPA2 et voir d'une part comment les déployer et d'autre part comment elles fonctionnent. Nous verrons qu'elles mettent en œuvre un cryptage puissant (TKIP ou AES), un mécanisme permettant d'assurer la distribution et la protection des clés de cryptage, un contrôle d'intégrité puissant et une bonne résistance aux attaques de relecture.

Un bémol toutefois : une faille a été découverte dans le système de contrôle d'intégrité du TKIP. Il ne signe pas immédiatement son arrêt de mort, mais il est tout de même recommandé de passer à l'AES dès que possible.

9.1 DÉPLOYER LE WPA OU LE WPA2

9.1.1 Rappels et définitions

Comme nous l'avons vu dans le chapitre 6 (§ 6.4), le groupe de travail 802.11i de l'IEEE a été mis en place pour développer une solution de sécurité nettement plus sûre

que la solution WEP définie dans la première version de la norme 802.11, dès 1997. Le WEP souffre en effet de nombreuses failles qui le rendent peu recommandable, comme nous l'avons vu au chapitre 7.

Malheureusement, entre la découverte des failles du WEP et la finalisation de la norme 802.11i, il s'est écoulé plusieurs années. En 2002, la WiFi Alliance a donc publié une solution de sécurité appelée *Wireless Protected Access* (WPA), qui est un sous-ensemble du 802.11i. La norme 802.11i a été ratifiée en juin 2004. La WiFi Alliance a alors créé la certification WPA2 pour les produits respectant la norme 802.11i au complet.

Un réseau qui repose uniquement sur le 802.11i (WPA ou WPA2) s'appelle un *Robust Security Network* (RSN), c'est-à-dire un « réseau à sécurité robuste ». Certains désignent donc le 802.11i sous le nom de RSN. Un réseau reposant à la fois sur le WEP et le 802.11i s'appelle un *Transitional Security Network* (TSN), c'est-à-dire un « réseau à sécurité transitionnelle ».

Le WPA et le WPA2 sont identiques du point de vue de leur architecture globale et donc de leur mise en œuvre. Le WPA repose sur un algorithme de cryptage défini par le protocole *Temporal Key Integrity Protocol* (TKIP), lui-même basé sur l'algorithme RC4 (que nous avons vu au chapitre 7, § 7.2), alors que le WPA2 repose, au choix, sur le TKIP ou sur un autre algorithme de cryptage appelé *Advanced Encryption Standard* (AES). Le WPA2 offre donc le choix du cryptage, contrairement au WPA qui impose TKIP.

Une autre différence importante est que le WPA n'est compatible qu'avec les réseaux de type Infrastructure (voir le chapitre 3) et non les réseaux Ad Hoc. Quant au WPA2, il peut sécuriser les deux types de réseau. Toutefois, vues les similitudes entre le WPA et le WPA2 et vu le succès commercial du WPA (apparu deux ans avant le WPA2), de nombreux produits WPA2 sont présentés simplement sous l'étiquette WPA. Si votre équipement « WPA » gère l'AES, il s'agit en fait d'un produit WPA2 et il gérera donc vraisemblablement aussi le mode Ad Hoc.

> Le WPA ne gère que le cryptage TKIP, qui est beaucoup plus sûr que le WEP. Le WPA2 gère le cryptage TKIP, mais aussi le cryptage AES, plus puissant encore.

Avant d'étudier les rouages internes du WPA et du WPA2, commençons par voir comment on les déploie. Il existe deux architectures pour le WPA ou le WPA2 :

- avec des clés partagées : on parle de « WPA Personal » ;
- avec une architecture 802.1x : on parle de « WPA Enterprise ».

9.1.2 Le WPA Personal

Pour déployer une sécurité WPA ou WPA2, le mécanisme le plus simple consiste à utiliser une clé partagée, ou *Pre-Shared Key* (PSK), configurée dans le poste de chaque utilisateur et dans chaque AP. Cette solution repose donc sensiblement sur le même principe que le WEP : le partage d'une même clé par tous les équipements.

Toutefois, alors que le WEP imposait de saisir la clé elle-même, en général au format hexadécimal, le WPA et le WPA2 offrent une méthode plus pratique : il faut saisir un mot de passe (aussi long que possible), appelé la « passphrase » et cette *passphrase* est passée automatiquement au travers d'une « moulinette » pour générer la PSK (fig. 9.1).

C'est tout, la sécurité est en place ! La PSK est de loin la solution la plus simple pour mettre en œuvre le WPA. C'est une solution recommandée pour les particuliers ou les très petites entreprises car elle ne suppose l'installation d'aucun serveur d'authentification et elle offre un niveau de sécurité bien supérieur au WEP.

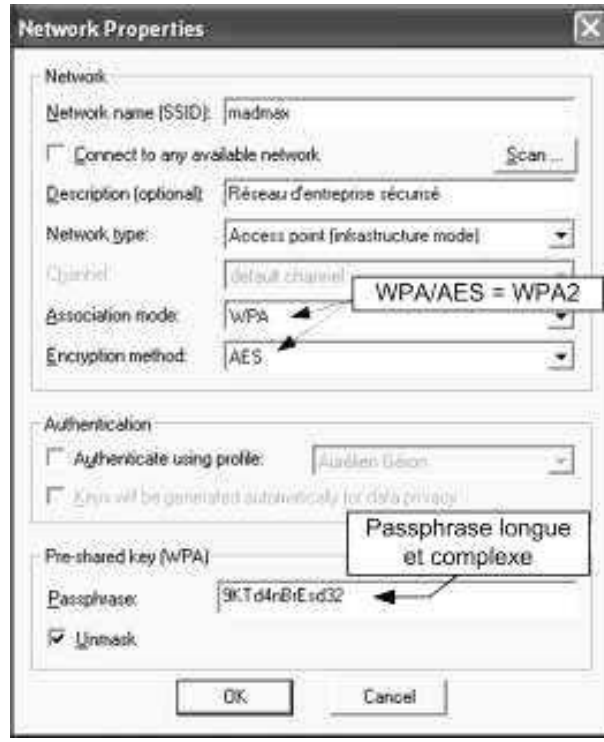


Figure 9.1 — Configuration WPA2 en mode PSK avec le logiciel de connexion Odyssey.

Malheureusement, la PSK a trois défauts :

- si le mot de passe choisi est trop court, un pirate peut lancer une attaque de dictionnaire hors-ligne pour le retrouver. Un mot de passe d'une vingtaine de caractères est recommandé, ou une douzaine de caractères s'il s'agit de lettres parfaitement aléatoires (ce qui est pénible à retenir) ;
- tous les utilisateurs partagent la même clé, ce qui augmente le risque qu'elle soit compromise et permet à tous les utilisateurs (qui possèdent la PSK) d'espionner le trafic des autres utilisateurs ;

- enfin, dès que le nombre d'utilisateurs augmente, ce système devient lourd à gérer car si l'on doit changer la clé, il faut reconfigurer tous les postes et tous les AP. En outre, aucun mécanisme de rotation de la clé PSK n'est prévu (contrairement au WEP, comme nous l'avons vu), ce qui ne facilite pas les choses.

La solution PSK est de loin la plus simple à mettre en place, mais elle ne convient que pour les petits réseaux Infrastructure ou les réseaux Ad Hoc. Il est indispensable de choisir une passphrase longue et complexe, et de la changer régulièrement.

9.1.3 Le WPA Enterprise

L'installation en deux mots

La méthode recommandée pour déployer le WPA ou le WPA2 est d'utiliser l'architecture 802.1x que nous avons décrite au chapitre précédent. Concrètement, cela signifie que vous devez :

- installer et configurer un serveur RADIUS[1] compatible avec l'EAP ;
- activer la gestion du 802.1x et du WPA (ou du WPA2) dans tous les AP. Dans le cas du WPA2, il faut choisir la méthode de cryptage : TKIP ou AES. Si tous les équipements le permettent, il vaut bien mieux utiliser l'AES, qui est un algorithme plus puissant. Certains AP sont capables de gérer les deux à la fois ce qui peut être utile si vos stations ne gèrent pas toutes l'AES ;
- configurer la connexion 802.1x et le WPA (ou le WPA2) sur le poste de chaque utilisateur. Bien entendu, il faut configurer le poste pour qu'il utilise le même algorithme de cryptage que les AP ;
- choisir une ou plusieurs méthodes d'authentification EAP, et les configurer dans le serveur RADIUS et dans l'interface de connexion des utilisateurs (fig. 9.2).

Cette solution est donc plus complexe et plus longue à mettre en œuvre, mais elle offre un niveau de sécurité très élevé, pourvu que l'on évite les quelques failles du 802.1x. Pour plus de détails sur le 802.1x et les méthodes EAP, consultez le chapitre 8. Pour la configuration du serveur RADIUS, voir le chapitre suivant.

Les méthodes génératrices de clés

L'un des avantages de la solution WPA Enterprise sur le 802.1x seul est que les clés de cryptage sont distribuées automatiquement, ce qui simplifie considérablement la gestion du système (une fois qu'il est mis en place). En outre, ces clés de cryptage sont différentes pour chaque utilisateur et pour chaque session, et peuvent même changer automatiquement en cours de session, comme nous le verrons plus bas. Ceci permet de garantir une sécurité bien plus élevée qu'avec des clés partagées.

1. Nous parlerons uniquement des serveurs d'authentification de type RADIUS. En effet, ils sont de loin les plus répandus, et le WPA impose ce type de serveur. Quant au WPA2, il laisse le choix ouvert.

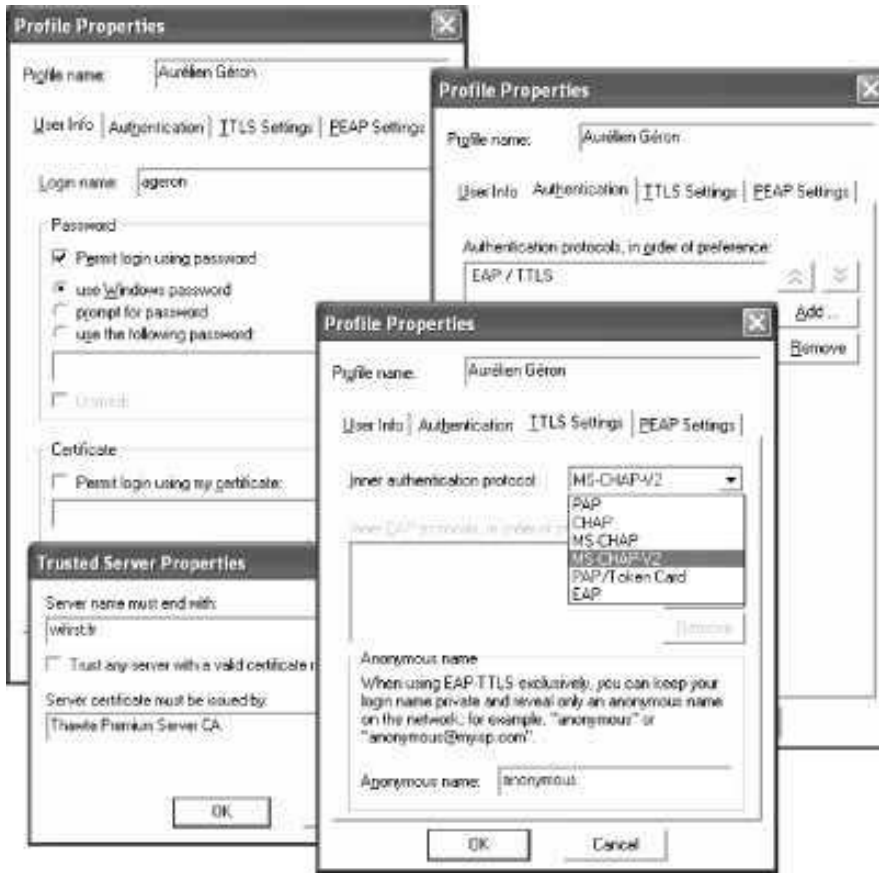


Figure 9.2 — Configuration d'un profile d'authentification 802.1x avec le logiciel Odyssey.

Il existe toutefois une contrainte imposée par le WPA et le WPA2 : si l'on veut bénéficier de la distribution automatique des clés de cryptage, la méthode EAP utilisée doit être capable de générer une clé secrète entre le client et le serveur d'authentification. Si c'est le cas, on dit que la méthode est « génératrice de clés » (*Key Generating*).

Toutes les méthodes à base de tunnels TLS sont génératrices de clés (encore une raison de plus pour les utiliser). En effet, nous avons vu qu'au cours de l'authentification avec ces méthodes, une clé secrète était d'abord générée par le client, puis cryptée à l'aide de la clé publique du serveur d'authentification et enfin envoyée au serveur. De même, la méthode EAP/FAST est génératrice de clés. Cette clé secrète peut alors servir de base pour la négociation sécurisée de clés de cryptage temporaires, comme nous le verrons au § 9.2.

Malheureusement, les méthodes simples, EAP/MD5, EAP/MS-CHAP-v2, EAP/OTP ou encore EAP/GTC, ne sont pas génératrices de clés. Si l'on utilise une telle méthode d'authentification, alors il est impossible d'utiliser la fonction de

distribution automatique des clés de cryptage. Dans ce cas, on est obligé de s'en tenir à une clé partagée (PSK)... et c'est bien dommage ! En effet, quitte à mettre en place une architecture 802.1x, autant qu'elle permette la distribution automatique des clés de cryptage. Il est donc très fortement recommandé d'utiliser une méthode génératrice de clés.

Par exemple : EAP/TLS, TTLS, PEAP, EAP/FAST.

Les méthodes TTLS, PEAP et EAP/FAST peuvent être utilisées avec n'importe quelle méthode d'authentification interne.

> La difficulté de la solution 802.1x réside surtout dans l'installation et la configuration du serveur RADIUS. Cependant, une fois que cette architecture est mise en place, elle est beaucoup plus facile à administrer et beaucoup plus sûre que le WEP, le WPA-PSK ou le WPA2-PSK.

À ce stade, vous avez déjà toutes les informations qu'il vous faut pour choisir la méthode EAP la mieux adaptée à vos besoins, configurer les AP et les logiciels de connexion des utilisateurs... et il ne vous reste plus qu'à apprendre comment installer et configurer un serveur RADIUS, ce que nous verrons au prochain chapitre.

Nous allons maintenant aborder le détail du fonctionnement du WPA et du WPA2. Si ce détail ne vous intéresse pas, vous pouvez dès maintenant passer au chapitre 10.

9.2 LA DISTRIBUTION DES CLÉS

9.2.1 Une connexion complète

Admettons qu'un utilisateur ait configuré son logiciel de connexion WiFi (le « client ») pour utiliser le WPA Enterprise. Que se passe-t-il lorsqu'il cherche à se connecter au réseau ? Il y a trois étapes : l'association WiFi, l'authentification 802.1x et la négociation des clés temporaires entre le client et l'AP.

L'association WiFi (fig. 9.3)

- le client détecte l'AP le plus proche dont le SSID est celui qu'il a sélectionné ;
- il envoie alors une requête d'authentification. Puisque, avec le WPA et le WPA2, l'AP devrait toujours être en mode « ouvert » et jamais en mode « d'authentification WEP », l'AP répondra simplement que l'authentification est réussie (au sens WiFi, pas au sens 802.1x) ;
- le client envoie une requête d'association à l'AP. Puisque l'authentification est réussie, l'AP accepte l'association. Bien qu'à ce stade l'utilisateur soit associé à l'AP, ce dernier ne le laisse pas encore accéder au réseau s'il respecte le protocole 802.1x.

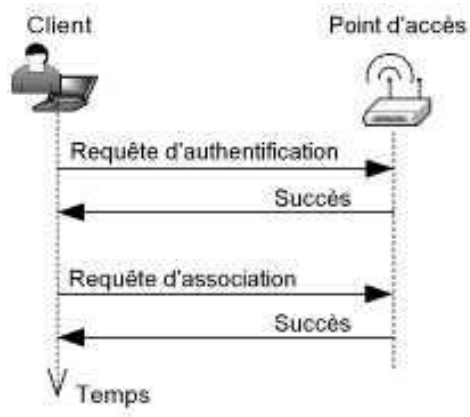


Figure 9.3 — L'association WiFi.

L'authentification 802.1x (fig. 9.4)

- le poste de l'utilisateur envoie maintenant une requête EAPoL-Start à l'AP, ce qui démarre une séquence d'échanges 802.1x pendant laquelle l'utilisateur doit être authentifié auprès du serveur d'authentification ;
- au cours de l'authentification, si la méthode utilisée est bien génératrice de clé, le client et le serveur se mettent d'accord secrètement sur une clé de 256 bits (32 octets), dérivée de la clé secrète générée par l'authentification : on l'appelle la *Pairwise Master Key* (PMK) ;
- le serveur d'authentification transmet la PMK à l'AP, à l'aide d'un paquet RADIUS prévu à cet effet. De cette façon, le client et l'AP possèdent tous deux la même clé PMK, qui leur permettra d'établir entre eux un tunnel sécurisé ;
- si le client est bien authentifié, le serveur lui envoie un paquet EAP de type Succès, que le contrôleur d'accès voit passer. Du point de vue du protocole 802.1x, l'affaire est close. Mais il reste encore quelques détails à régler avant que le client puisse se connecter au réseau.

Négociation des clés temporaires (fig. 9.5)

- le client et l'AP se mettent maintenant d'accord sur une nouvelle clé dérivée de la clé PMK : cette clé temporaire s'appelle la *Pairwise Transient Key* (PTK). Ce faisant, ils en profitent pour vérifier qu'ils possèdent bien la même clé de départ PMK. Dorénavant, tous leurs échanges sont cryptés avec la clé PTK : un tunnel sécurisé est en place ;
- grâce à ce tunnel, l'AP peut envoyer secrètement au client la clé qu'il utilise pour crypter le trafic broadcast et multicast : la *Group Transient Key* (GTK). Il le fait en utilisant un paquet EAPoL-Key contenant la GTK cryptée. Maintenant, le client peut également décrypter le trafic de groupe ;
- après tous ces efforts, le client peut enfin accéder au réseau : toutes ses communications sont bien cryptées !

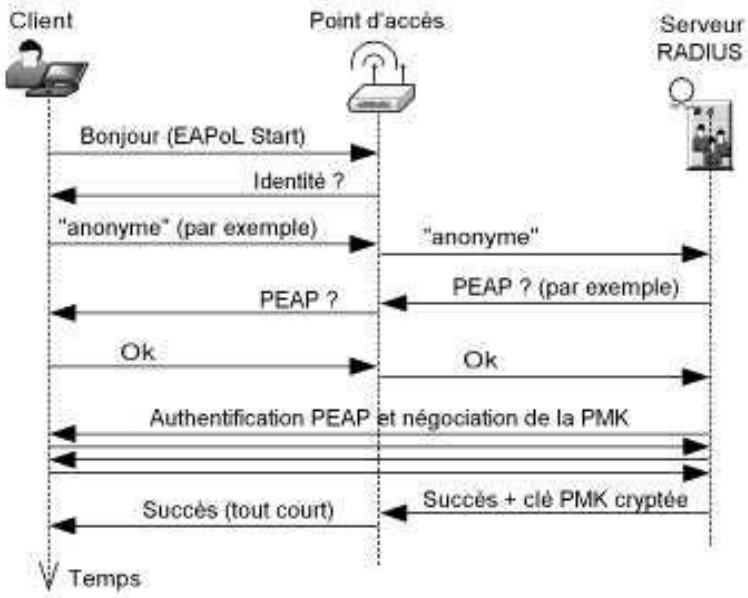


Figure 9.4 — L'authentification 802.1x.

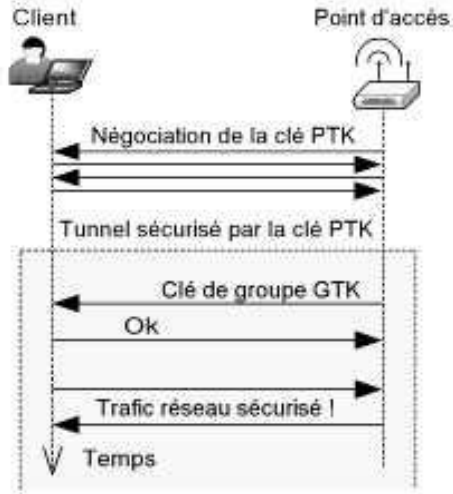


Figure 9.5 — La négociation des clés temporaires.

9.2.2 La hiérarchie des clés

Clés maîtresses et clés dérivées

Nous venons de voir le détail d'une connexion complète avec le WPA (ou le WPA2) Enterprise. Plusieurs clés ont été mentionnées :

- la clé maîtresse **PMK**, négociée au cours de l'authentification. *Note* : si l'on utilise la solution de la clé partagée à l'avance (PSK), plutôt que l'architecture 802.1x, alors la clé PSK est simplement utilisée comme clé PMK ;
- la clé temporaire **PTK**, dérivée de la PMK ;
- la clé temporaire de groupe **GTK**, générée par l'AP.

En réalité, lorsque l'AP décide de générer une nouvelle clé de groupe, il génère d'abord aléatoirement une clé de 128 bits appelée la *Group Master Key* (GMK). Il dérive ensuite la GTK à partir de la GMK. Il y a donc quatre clés principales (fig. 9.6) : la PMK, la PTK, la GMK et la GTK.

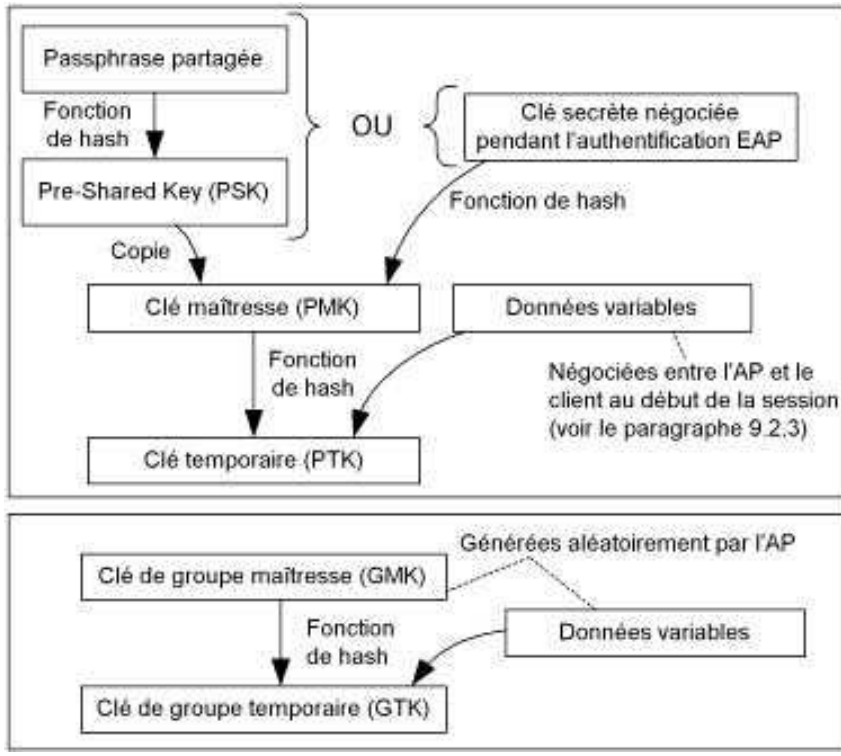


Figure 9.6 — La hiérarchie des clés du WPA et du WPA2.

La raison pour laquelle une clé temporaire (PTK) est dérivée à partir de la clé maîtresse (PMK) est que cela permet d'éviter que la PMK soit directement utilisée pour les opérations de cryptage, ce qui la rendrait potentiellement vulnérable à des attaques. En utilisant plutôt une clé dérivée de la clé maîtresse, on contribue à protéger

cette dernière. En revanche, le fait de dériver une clé GTK à partir de la clé GMK n'a pas grand intérêt puisque la clé GMK est elle-même générée aléatoirement et remplacée régulièrement. Mais ça ne fait pas de mal non plus !

> Les clés maîtresses PMK et GMK ne sont pas utilisées directement : des clés temporaires, « fraîches », sont dérivées à chaque session et utilisées pour le cryptage et le contrôle d'intégrité des messages. Ce mécanisme permet de protéger les clés maîtresses.

Clés de cryptage et clés d'intégrité

Pour compliquer encore un peu les choses, les clés temporaires sont elles-mêmes découpées en morceaux pour donner de nouvelles clés. Ceci s'explique par le fait qu'il y a deux fonctions pour lesquelles des clés sont nécessaires : le cryptage et le contrôle d'intégrité des paquets. Nous verrons cela plus bas en détaillant les algorithmes TKIP et AES. La dérivation des clés temporaires à partir de la PMK et de la GMK varie selon qu'on utilise TKIP ou AES.

Pour TKIP

Par le biais d'un dialogue entre le client et l'AP (que nous étudierons au § 9.2.3), une PTK de 512 bits est dérivée de la PMK de 256 bits. La PTK est composée de quatre clés de 128 bits chacune, ayant toute un rôle différent :

PTK			
Intégrité EAPoL	**Cryptage EAPoL**	**Cryptage du tunnel**	**Intégrité du tunnel**
128 bits	128 bits	128 bits	128 bits

Les deux premières clés servent à protéger le trafic EAPoL entre le client et l'AP. Les deux dernières servent à protéger le reste du trafic entre le client et l'AP : ce sont les clés les plus utilisées.

La GTK de 256 bits est dérivée à partir de la GMK de 128 bits, simplement en utilisant un algorithme de *hash*[1]. Elle est composée de deux clés de 128 bits chacune :

GTK	
Cryptage des données	**Intégrité des données**
128 bits	128 bits

Comme nous l'avons vu, la clé GTK sert à protéger le trafic broadcast et multicast envoyé par l'AP. Rappelons qu'en mode Infrastructure, ce type de trafic est toujours

1. En plus de la GMK, un *nonce* (numéro unique) et l'adresse MAC de l'AP sont également utilisés pour générer la GTK, mais cela n'a pas grande importance car la GMK est déjà un nombre aléatoire.

émis par un AP. En effet, lorsque le client veut envoyer un paquet broadcast ou multicast, ce paquet est d'abord envoyé strictement à l'AP, qui se charge ensuite de l'émettre vers tout le monde. Seul l'AP émet donc des paquets à plusieurs personnes à la fois. La GTK ne sert donc qu'à la réception pour les clients et à l'émission pour l'AP. Nous verrons plus bas comment cela se passe en mode Ad Hoc.

Pour AES

Avec l'AES, la même clé peut être utilisée pour le cryptage et pour le contrôle d'intégrité. Les clés PTK et GTK sont donc plus courtes que celles que nous venons de voir pour le TKIP. La PTK, de 384 bits, est composée de trois clés de 128 bits chacune :

PTK		
Intégrité EAPoL	**Cryptage EAPoL**	**Cryptage et intégrité**
128 bits	128 bits	128 bits

Comme précédemment, les deux premières clés servent à protéger le trafic EAPoL. La dernière clé sert à la fois au cryptage et au contrôle d'intégrité pour le reste du trafic entre le client et l'AP.

La GTK, quant à elle, n'a plus qu'une longueur de 128 bits. Elle n'est composée que d'une seule clé, qui sert à la fois au cryptage et au contrôle d'intégrité du trafic de groupe envoyé par l'AP :

GTC
Cryptage et intégrité
128 bits

9.2.3 Dérivation de la clé temporaire PTK

Intérêts de la dérivation

Résumons : la clé maîtresse PMK peut être obtenue de deux façons différentes :

- soit une passphrase est saisie directement dans chaque équipement et sert à générer la clé partagée PSK. Cette clé PSK est alors utilisée directement comme clé PMK ;
- soit la PMK est secrètement échangée entre le client et le serveur au cours de l'authentification 802.1x, pourvu que la méthode utilisée soit génératrice de clé. Dans ce cas, le serveur n'a plus qu'à envoyer cette clé à l'AP, au sein d'un paquet RADIUS.

Une fois que le client et l'AP possèdent la même clé PMK et que l'authentification est terminée, il reste à dériver la clé temporaire PTK à partir de la clé PMK. Pour

cela, le client et l'AP s'échangent une série de quatre messages, dans des paquets EAPoL-Key. Cet échange a deux objectifs :

- que le client et l'AP génèrent une même clé temporaire PTK. Celle-ci doit être différente à chaque session, même si la clé PMK ne change pas (comme c'est le cas si l'on utilise une clé partagée, saisie manuellement) ;
- s'assurer que le client et l'AP partagent bien la même clé PMK. Cela doit normalement être le cas si un pirate n'a pas modifié des paquets échangés auparavant.

La négociation de la PTK

La clé temporaire PTK est générée grâce à une fonction de *hash* (qu'il serait inutile de détailler ici) à partir de cinq valeurs :

- la clé maîtresse PMK ;
- un *nonce*, c'est-à-dire un numéro censé n'être utilisé qu'une seule fois, généré par le client ;
- un *nonce* généré par l'AP ;
- l'adresse MAC du client ;
- l'adresse MAC de l'AP.

Le client et l'AP connaissent déjà la clé PMK, ainsi que leur propre adresse MAC et celle de l'autre et ils peuvent chacun générer leur propre *nonce*. Bref, il ne leur manque que le *nonce* de l'autre pour pouvoir générer la clé PTK. Voici comment ils procèdent pour se l'échanger avec des paquets EAPoL-Key et en profiter pour vérifier qu'ils possèdent tous deux la même clé PMK (fig. 9.7) :

- L'AP envoie son *nonce* au client, en clair.
- Le client génère la clé PTK car il possède maintenant tous les éléments pour le faire. Il envoie ensuite à l'AP son propre *nonce*, en rajoutant un code de contrôle d'intégrité généré grâce à la clé d'intégrité EAPoL (la première clé contenue dans la PTK).
- Grâce au *nonce* du client, l'AP peut maintenant lui aussi générer la clé PTK. Il utilise cette clé pour vérifier le code d'intégrité envoyé par le client. Si ce code est bon, l'AP sait que le client possède la bonne clé PMK (sinon, c'est l'échec de la connexion). Ensuite, il envoie un message au client pour lui an*noncer* que tout va bien et il rajoute un code d'intégrité à ce message. Il indique également le compteur à partir duquel les paquets devront être numérotés (nous y reviendrons).
- Le client peut contrôler le code d'intégrité de l'AP et s'assurer ainsi que l'AP possède bien la bonne clé PMK. Il envoie enfin un message à l'AP pour lui dire qu'il est prêt à démarrer la session.

Ces quatre messages forment ce qu'on appelle le *four-way handshake* (littéralement, la « poignée de main à quatre sens »). Comme prévu, ces quatre étapes permettent au client et à l'AP de négocier une clé PTK originale, tout en leur assurant que l'autre

possède bien la bonne clé PMK. Après le dernier message envoyé par le client, les deux cryptent dorénavant tous leurs messages.

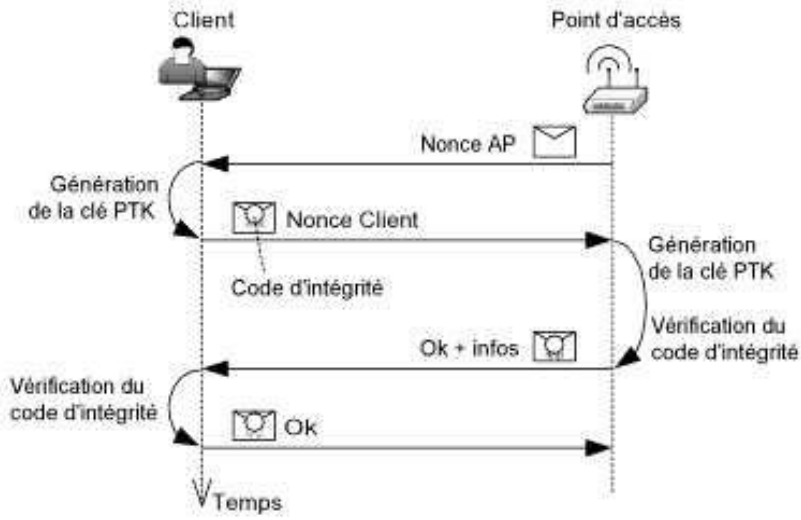


Figure 9.7 — Négociation de la clé temporaire PTK avec le *four-way handshake*.

Comme nous l'avons dit plus haut, l'AP envoie maintenant au client la clé de groupe temporaire GTK en cours. Puisqu'il y a désormais une connexion sécurisée entre le client et l'AP, la GTK est simplement envoyée telle quelle dans ce tunnel.

La pré-authentification

Le mécanisme d'authentification et de distribution des clés a été critiqué pour sa lourdeur : en général, le tout ne prendra que quelques fractions de secondes, mais pour certains systèmes et selon le type d'authentification choisi, cela peut prendre jusqu'à quelques secondes, par exemple si le serveur d'authentification est chargé ou si l'adaptateur du client (ou de l'AP) est peu puissant. Cette lenteur relative n'est pas très grave si le client ne se reconnecte pas très fréquemment : un utilisateur peut bien patienter une ou deux secondes pour se connecter ! Toutefois, cela peut poser des problèmes si le client se déplace d'une cellule à une autre, car dans ce cas il doit s'authentifier à nouveau et renégocier les clés temporaires : bref, tout est à refaire. Ceci peut poser problème, par exemple si l'utilisateur est en conversation téléphonique en voix sur IP (VoIP) : au moment d'un changement de cellule, sa conversation sera suspendue le temps que la nouvelle authentification ait lieu.

Pour limiter ce problème, le WPA suggère un nouveau mécanisme : la pré-authentification. Admettons qu'un utilisateur soit déjà connecté au réseau par le biais d'un AP (l'AP « de départ ») et qu'il se déplace vers la zone de couverture d'un autre AP (l'AP « d'arrivée »). La pré-authentification consiste à lancer le processus d'authentification auprès de l'AP d'arrivée *avant* de quitter l'AP de départ. Tous

les paquets 802.1x nécessaires à cette nouvelle authentification passent par l'AP de départ et le système de distribution (le réseau local) pour atteindre l'AP d'arrivée. De cette façon, au moment où la nouvelle authentification se termine, le client peut se désassocier de l'AP de départ et se réassocier à l'AP d'arrivée : l'authentification est déjà faite et il ne perd donc pas de temps.

9.2.4 La rotation de la clé de groupe

Au cours de la session, l'AP peut régulièrement changer de clé GTK. L'intervalle de temps entre les changements de clés peut en général être configuré dans l'AP. En outre, il peut décider de changer la clé GTK à chaque fois qu'un utilisateur rejoint ou quitte le réseau, afin d'éviter que cet utilisateur puisse décrypter le trafic de groupe antérieur ou postérieur à sa connexion.

Lorsqu'il change sa clé GTK, l'AP doit la fournir aux clients qui lui sont associés, afin qu'ils puissent continuer à décrypter le trafic de groupe. Si l'AP envoie cette nouvelle clé GTK par un simple broadcast crypté avec l'ancienne clé GTK, cela n'aura aucun intérêt puisque les utilisateurs déconnectés, mais possédant encore l'ancienne clé GTK, pourront obtenir la nouvelle clé GTK. En outre, certains clients risqueraient de ne pas recevoir la nouvelle clé, s'il y a une interférence au moment de la transmission, par exemple. Pour ces raisons, la nouvelle clé GTK est envoyée par l'AP à chaque client, un par un, en utilisant le tunnel établi avec lui.

Puisque ceci peut prendre du temps et que l'on ne peut pas bloquer le réseau pour autant, un mécanisme doit permettre de réaliser une transition douce. Pour cela, le principe de rotation de clé du WEP est réutilisé pour cette rotation de clé de groupe (fig. 9.8) :

- l'AP génère d'abord la nouvelle clé de groupe mais il ne l'utilise pas encore ;
- il envoie cette nouvelle clé GTK à chaque client, un par un, à l'aide d'un paquet EAPoL-Key crypté différemment pour chaque client ;
- lorsqu'un client reçoit la nouvelle clé GTK, il la rajoute dans sa liste de clés GTK utilisables et renvoie une confirmation de réception ;
- dès que l'AP a donné la nouvelle clé à tout le monde, il se met à l'utiliser.

Grâce à ce système, la clé GTK peut changer régulièrement sans que cela n'interompe les communications.

9.2.5 Le fonctionnement en mode Ad Hoc

Négociation de la clé PTK

Comme le WEP, le WPA2 est utilisable en mode Ad Hoc (mais pas le WPA). Seule l'utilisation d'une clé partagée (PSK) est envisageable. Du point de vue de l'utilisation, il n'y a rien de spécial à ajouter : chaque utilisateur configure son poste à l'aide de la passphrase, ce qui génère la clé maîtresse (PMK) et permet ainsi le cryptage des communications.

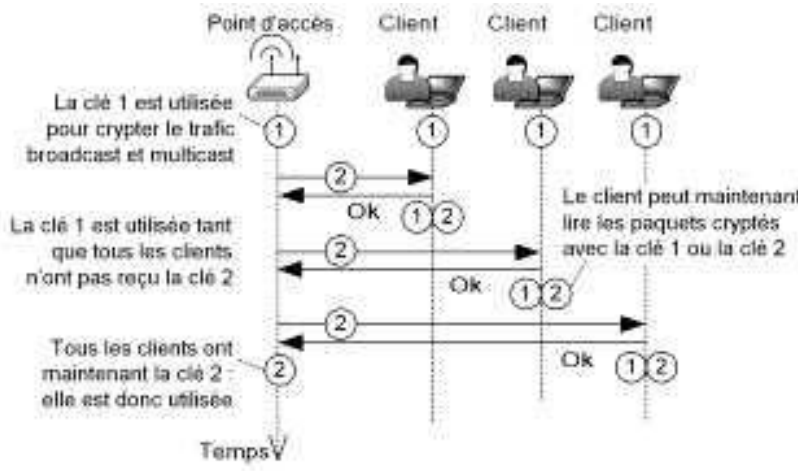


Figure 9.8 — La rotation automatique de la clé de groupe GTK.

C'est tout : si l'utilisateur a bien configuré son poste en mode Ad Hoc (et a configuré son adressage IP), il n'a en général pas besoin de se soucier d'autre chose.

En revanche, le mécanisme de négociation des clés temporaires, PTK et GTK, est légèrement différent de celui que nous avons vu pour le mode Infrastructure.

En mode Ad Hoc, lorsque deux stations doivent communiquer entre elles, avec la sécurité WPA2-PSK, elles commencent par dériver une clé temporaire PTK à partir de la clé maîtresse PMK. Pour cela, elles suivent le mécanisme *four-way handshake* que nous avons décrit précédemment (la station dont l'adresse MAC est la plus basse commence). Ceci permet aux deux stations de négocier une clé temporaire PTK et de s'assurer que l'autre possède bien la bonne clé maîtresse PMK. Dorénavant les deux stations peuvent communiquer l'une avec l'autre en cryptant toutes leurs communications. Voyons maintenant comment se déroule la négociation des clés de groupes GTK.

Négociation de la clé GTK

En mode Ad Hoc, chaque station peut envoyer directement des paquets de groupe (broadcast ou multicast), alors qu'en mode Infrastructure ces paquets doivent d'abord être envoyés à l'AP, qui se charge lui-même de les diffuser. Du coup, la négociation des GTK est plus complexe en mode Ad Hoc qu'en mode Infrastructure (fig. 9.9) :

- chaque station génère sa propre GMK et en dérive sa propre GTK ;
- dès que deux stations se rencontrent, elles négocient une clé temporaire PTK, comme nous venons de le voir. À l'issue de cette négociation, les deux stations s'échangent alors secrètement leurs clés de groupe temporaires GTK respectives, en les cryptant à l'aide de la PTK qu'elles viennent de négocier.

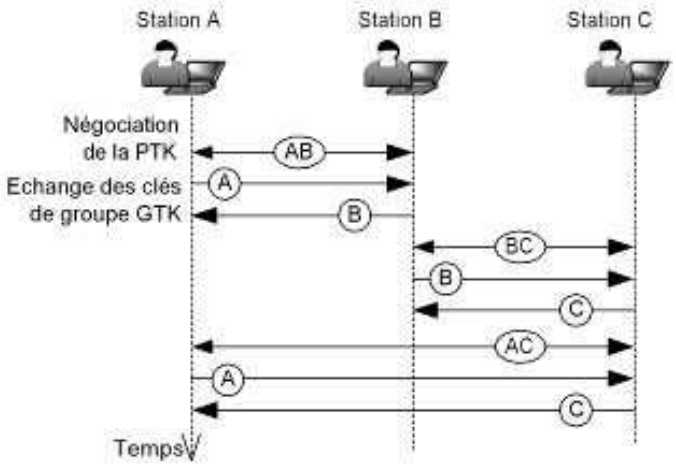


Figure 9.9 — La négociation des clés en mode Ad Hoc.

Un grand nombre de clés

Avec les mécanismes que nous venons de voir, il apparaît que dans un réseau comptant n stations qui communiquent toutes entre elles, chaque station doit retenir $n - 1$ clés PTK et n clés GTK ! Au total, les stations du réseau utilisent $n - (n - 1) / 2$ clés PTK différentes et n clés GTK.

Par exemple, pour un réseau Ad Hoc composé de 20 stations, pas moins de 190 clés PTK différentes sont négociées, plus 20 clés GTK différentes ! Rappelons qu'en mode Infrastructure, chaque station ne doit retenir que deux clés : la PTK et la GTK, plus éventuellement la nouvelle clé GTK lors de la rotation de la clé de groupe.

Bref, cette solution fonctionne bien, tant que le nombre de stations reste faible. Ceci dit, puisque seules les stations situées à portées les unes des autres peuvent communiquer ensemble, en mode Ad Hoc, le nombre de clés n'est sans doute pas un problème dans la majorité des contextes.

Nous avons maintenant présenté l'ensemble des mécanismes de gestion des clés mis en œuvre par le WPA et le WPA2 : l'obtention de la clé maîtresse PMK (clé partagée ou 802.1x), la dérivation des clés temporaires GTK et PTK et enfin leur distribution. Voyons maintenant comment la solution TKIP (*Temporal Key Integrity Protocol*) réalise le cryptage des données et le contrôle d'intégrité. Nous passerons ensuite à l'AES.

9.3 LA SOLUTION TKIP

9.3.1 Présentation générale

Les objectifs de TKIP

La solution de sécurité *Temporal Key Integrity Protocol* (TKIP) a été introduite avec le WPA en 2002, en réponse aux défaillances de sécurité du WEP. Sa conception a été dictée par deux impératifs :

- offrir un niveau de sécurité aussi élevé que possible ;
- faire en sorte que le matériel n'ait pas à être remplacé pour le gérer.

Toute la conception de TKIP a donc été marquée par ce compromis. L'objectif était simplement d'avoir une solution très sûre, utilisable sur les équipements WiFi de l'époque, et permettant d'attendre que l'AES soit très répandu. Le TKIP a parfaitement rempli son rôle car aucune faille n'y a été découverte de 2002 à fin 2008. Or, l'AES est disponible depuis 2004, et depuis 2006 la WiFi Alliance impose le support de l'AES dans tous les produits certifiés : à moins que votre matériel ne soit vraiment très ancien, il est fort probable que vous puissiez d'ores et déjà passer à l'AES.

Il est donc sans doute temps de remercier TKIP, et de passer à l'AES. Il ne va pas falloir trop tarder d'ailleurs car malheureusement une première faille de sécurité a été découverte dans le système de contrôle d'intégrité « Michael » sur lequel repose TKIP (cf. § 9.3.4).

> Bien que la faille découverte dans le protocole d'intégrité du TKIP soit encore difficile à exploiter et qu'elle ait des conséquences encore relativement limitées, il est désormais fortement conseillé de quitter le TKIP et de passer à l'AES.

Les nouveautés de TKIP

Pour comprendre le fonctionnement de TKIP, le plus simple est de le comparer au WEP. Nous vous invitons donc à lire le chapitre 7 maintenant si vous ne l'avez pas déjà fait : il vous apprendra les rouages du WEP. Voici les principales modifications apportées par TKIP par rapport au WEP :

- le contrôle d'intégrité repose sur le protocole Michael, qui remplace le contrôle d'intégrité (ICV) du WEP : ce protocole Michael a malheureusement été cassé fin 2008 ;
- le vecteur d'initialisation (*Initialisation Vector*, IV) est beaucoup plus long, 48 bits, contre 24 bits pour le WEP : ceci permet d'éviter complètement la réutilisation des clés RC4 ;
- un mécanisme permet d'éviter l'utilisation de clés RC4 faibles ;
- la clé de cryptage change à chaque paquet ;
- l'IV est également utilisé pour contrer les attaques de relecture ;
- les clés sont distribuées selon un mécanisme (que nous avons étudié au § 9.2.3) plus souple et plus sûr que celui du WEP (la distribution manuelle).

Nous allons maintenant détailler chacun de ces nouveaux mécanismes.

9.3.2 Le cryptage TKIP

Un cryptage très proche du WEP

Comme pour le WEP, le cryptage mis en œuvre par TKIP repose sur l'algorithme RC4. Rappelons en deux mots le principe de ce cryptage (détaillé au chapitre 7) :

- pour chaque paquet à envoyer, l'algorithme RC4 permet de calculer, à partir d'une clé RC4, une séquence de bits pseudo-aléatoires R, de même longueur que les données à crypter M ;
- le cryptage s'effectue simplement en combinant R et M grâce à l'opération « ou exclusif » (XOR), notée $\oplus$, qui est une addition bit par bit, sans retenue (c'est-à-dire que $1 \oplus 1 = 0$). Pour le message M = 1001 et une séquence pseudo-aléatoire R = 0011, par exemple, on obtient $C = M \oplus R = 1010$, qui est le message crypté à transmettre ;
- à l'arrivée, le récepteur utilise la même clé RC4 pour générer la même séquence de bits pseudo-aléatoires R et il retrouve le message original M grâce à l'opération : $M = C \oplus R$. Dans notre exemple : $M = 1010 \oplus 0011 = 1001$.

Le cryptage TKIP diffère du cryptage WEP uniquement par le choix de la clé RC4. Dans le cas du WEP, la clé RC4 était constituée d'un vecteur d'initialisation (IV) d'une longueur de 24 bits, suivi de la clé WEP de 40 ou 104 bits. L'IV changeait à chaque paquet et était envoyé en clair dans chaque paquet pour permettre au récepteur de reconstituer la clé RC4. L'IV avait pour but d'éviter que la même clé RC4 soit utilisée plusieurs fois, car alors les messages concernés peuvent être décryptés assez facilement.

> Avec le cryptage TKIP, la clé RC4 complète change pour chaque paquet envoyé.

La clé RC4

Un IV de 48 bits

L'IV utilisé dans le protocole TKIP a une longueur de 48 bits et il est simplement incrémenté à chaque paquet envoyé. Alors que toutes les valeurs possibles d'un IV de 24 bits (comme en WEP) peuvent être épuisées en quelques heures dans un réseau chargé, il faudrait plusieurs milliers d'années pour épuiser celles d'un IV de 48 bits. Ceci permet de garantir qu'une même clé RC4 ne sera jamais utilisée deux fois de suite par une même station.

Malheureusement, la plupart des adaptateurs WiFi ne peuvent pas être mis à jour pour accepter un IV d'une longueur différente de 24 bits. Pour cette raison, les 16 derniers bits de l'IV de TKIP sont combinés avec 8 bits (un octet) choisis de telle sorte que les clés RC4 faibles soient évitées (voir le chapitre 7), pour former un champ de 16 + 8 = 24 bits, qui prend la place de l'IV du WEP.

Le reste de la clé, auparavant occupé par la clé WEP qui ne changeait jamais, est maintenant modifié à chaque paquet à partir de l'IV au complet (les 48 bits), comme nous allons le voir.

Clé RC4 du WEP

IV	Clé WEP (statique)
24 bits	40 ou 104 bits

Clé RC4 de TKIP

16 derniers bits de l'IV + 8 bits contre les clés faibles	Partie changeante (à chaque paquet)
24 bits	104 bits

Transmission de l'IV

Avec le WEP, l'IV était envoyé en clair dans chaque paquet, entre l'en-tête MAC et les données cryptées. Ceci permettait au récepteur de reconstituer la clé RC4 à partir de l'IV et de la clé WEP pour pouvoir décrypter le message. Puisque le même matériel WiFi est utilisé pour le TKIP, le même mécanisme a lieu, ce qui permet au récepteur de récupérer les 16 derniers bits de l'IV. Mais comment récupère-t-il les 32 premiers bits ? La réponse est simple : ces 32 bits (4 octets) sont insérés juste avant les données cryptées[1]. Ils constituent ce qu'on appelle « l'IV étendu » (*Extended IV*) :

Paquet crypté avec le WEP

IV	ID	Données cryptées	ICV crypté
3 octets	1 octet	0 à 2 304 octets	4 octets

Paquet crypté avec TKIP

16 bits IV+...	ID	32 bits IV	Données cryptées	ICV crypté
3 octets	1 octet	4 octets	0 à 2 300 octets	4 octets

Le champ ID servait, avec le WEP, à indiquer laquelle des quatre clés WEP était utilisée (de 0 à 3). Le sixième bit ce champ sert maintenant à indiquer si le champ Extended IV est présent ou non. Avec TKIP, il est bien sûr toujours égal à 1 car l'Extended IV est toujours présent. Ceci est utile lorsque le WEP et le WPA sont tous les deux utilisés sur le même réseau (c'est le « mode mixte », voir § 9.3.5). Les deux derniers bits de cet octet forment l'identifiant de la clé, de 0 à 3. Avec le TKIP, cet identifiant est toujours égal à 0 si le trafic est unicast. Si le trafic est multicast ou

1. Malheureusement, certains adaptateurs WiFi ne peuvent pas être modifiés pour gérer ce changement et ils ne peuvent donc pas être mis à jour pour gérer la sécurité TKIP.

broadcast, il indique l'index de la clé GTK utilisée (voir la rotation de la clé de groupe, au § 9.2.4).

Notez que le même contrôle d'intégrité que celui du WEP est utilisé à ce niveau, avec le code ICV. Nous avons vu qu'il était relativement facile de le tromper, mais il ne fait pas de mal. Ce mécanisme est complété par le contrôle d'intégrité mis en œuvre par le protocole Michael, que nous verrons au § 9.3.4.

Calcul de la clé RC4

Grâce à l'IV de 48 bits, un même utilisateur n'aura jamais deux fois le même IV. Mais que se passe-t-il si deux stations commencent toutes les deux à compter l'IV à partir de zéro : ces deux stations utiliseront alors les mêmes IV, pour tous leurs paquets ! Pour éviter que cela n'aboutisse à la même clé RC4, TKIP utilise (entre autres) l'adresse MAC de la station émettrice pour générer la clé RC4. Grâce à cela, deux stations distinctes ne peuvent pas avoir la même clé RC4.

Plus précisément, le calcul de la clé RC4 se fait de la façon suivante (fig. 9.10) :

- les 24 premiers bits (anciennement l'IV du WEP) sont composés, comme nous l'avons vu, des 16 derniers bits de l'IV plus 8 bits choisis de telle sorte que les clés RC4 faibles soient évitées ;
- les 104 derniers bits (anciennement la clé WEP) sont le résultat de fonctions de *hash* appliquées sur l'IV au complet (48 bits), l'adresse MAC de l'émetteur et bien sûr la clé temporaire (PTK ou GTK, selon le type de trafic).

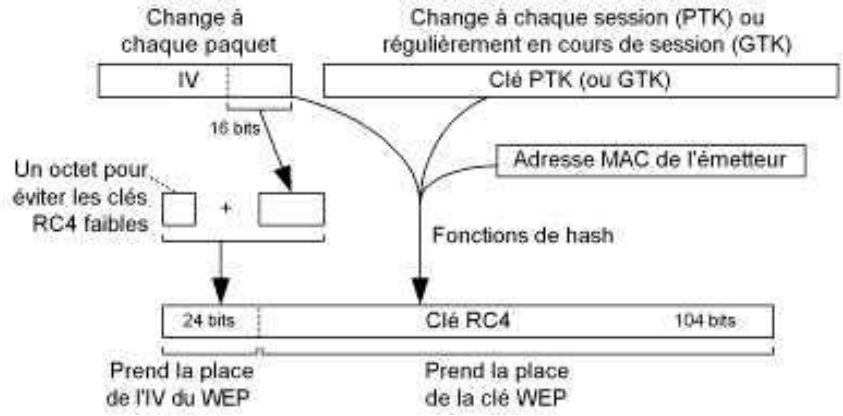


Figure 9.10 — Génération d'une nouvelle clé RC4 à chaque paquet.

Les principaux défauts du WEP sont éliminés par TKIP, grâce à la longueur de l'IV, la présence de l'octet permettant d'éviter les clés faibles et le changement du reste de la clé RC4, à chaque paquet.

9.3.3 Empêcher la relecture

L'un des problèmes du WEP est qu'un pirate peut facilement enregistrer un paquet et l'émettre à nouveau, à l'identique : le récepteur n'a alors aucun moyen de savoir si ce paquet est une copie ou non. Cela s'appelle une attaque de relecture et nous avons vu au chapitre 7 qu'une des attaques les plus graves contre le WEP reposait entre autres sur cette faille pour générer des requêtes *ping* à l'infini.

Pour éviter cela, TKIP utilise tout simplement l'IV pour identifier « l'âge du paquet ». Dans ce contexte, l'IV est appelé le compteur séquentiel TKIP (*TKIP Sequence Counter*, TSC), mais il s'agit bien du même nombre, composé de 48 bits.

Puisque le TSC (l'IV) est incrémenté à chaque paquet, il n'est pas difficile de savoir si un paquet est « vieux » ou non : il suffit qu'il ait un TSC plus petit ou égal que celui du dernier paquet (valide) reçu, que l'on notera TSCmax. La règle pourrait donc être : rejeter tout paquet avec un TSC inférieur ou égal à TSCmax.

Cependant, il se peut qu'un paquet soit envoyé deux fois de suite par une station (donc avec le même TSC) : ce sera le cas par exemple si elle ne reçoit pas le paquet ACK en réponse de son premier envoi, à cause d'interférences. Dans ce cas, le récepteur se rendra compte qu'il s'agit d'une répétition (d'autant que les paquets qui sont des répétitions sont marqués comme tel, comme nous l'avons vu au chapitre 3) et il pourra simplement conserver une seule copie du paquet et renvoyer un ACK à l'émetteur. Il ne faut donc pas forcément ignorer les paquets donc le TSC est égal à TSCmax : il peut s'agir de répétitions légitimes, auxquelles il faut répondre par un ACK.

Pour finir, il est important de noter une nouveauté introduite par le standard 802.11e[1] : jusqu'à 8 classes de services sont prévues, et chacune dispose de son propre compteur (TSC). Cela semble anodin, mais malheureusement ces 8 compteurs indépendants sont utilisés dans l'attaque contre le contrôle d'intégrité Michael, comme nous allons le voir dans le paragraphe suivant.

9.3.4 Le contrôle d'intégrité Michael

Le protocole Michael

Il reste un dernier volet à la sécurité TKIP : le contrôle d'intégrité, c'est-à-dire la possibilité pour le récepteur de s'assurer que le paquet qu'il reçoit n'a pas été modifié par un pirate.

Le contrôle d'intégrité de TKIP repose sur le protocole Michael, développé en 2002 par Neils Ferguson, justement pour TKIP. Ce protocole a été conçu pour répondre aux attentes exprimées par les concepteurs de la solution WPA : offrir une bonne sécurité sur le matériel existant. Michael a donc été conçu pour être très simple à mettre en œuvre, sûr et rapide. Sa simplicité permet de le rajouter dans un *firmware*

1. Rappelons que le standard 802.11e permet d'améliorer la qualité de service (QoS) en WiFi, et est mis en œuvre dans les produits certifiés WMM, comme nous l'avons vu au chapitre 3.

et sa rapidité permet au processeur de l'adaptateur WiFi de calculer sans problème un code d'intégrité pour chaque paquet, même si le trafic est important.

Le protocole Michael fonctionne en calculant un code d'intégrité de message (*Message Integrity Code*, MIC) de 64 bits à partir de la clé d'intégrité[1], de l'adresse MAC de destination, de l'adresse MAC de l'émetteur et enfin du message non crypté (fig. 9.11). Le détail de ce calcul a peu d'importance : il faut simplement savoir que c'est une fonction de *hash* constituée uniquement d'opérations simples à réaliser (addition, XOR, décalage de bits...), mais dont le résultat est un code très difficile à prévoir. Ce MIC est rajouté à la fin du message non crypté et est crypté avec lui, un peu comme le code ICV du WEP. Il y a cependant une différence importante : le protocole Michael travaille au niveau du MSDU et non du MPDU. En d'autres termes, il est calculé sur le message à envoyer, *avant* une éventuelle fragmentation (voir le chapitre 3, § 3.6.2) et est rajouté à celui-ci. À la réception, c'est donc après la reconstitution d'un MSDU à partir d'un ou plusieurs fragments (MPDU) que le code MIC peut être validé.

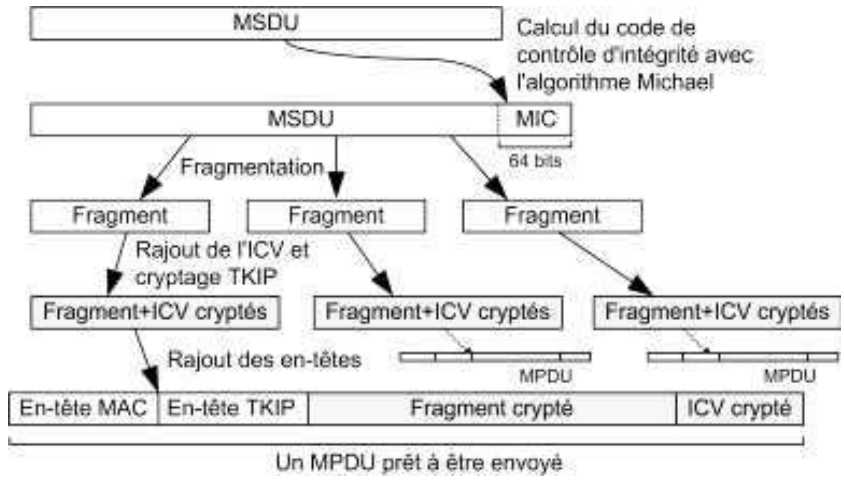


Figure 9.11 — Le contrôle d'intégrité Michael.

Puisque le MIC est rajouté aux données et qu'il est crypté avec elles, un pirate ne peut pas le modifier. Ceci dit, on pensait la même chose au sujet du code ICV du WEP et pourtant une simple opération permet de modifier l'ICV pour tromper le contrôle d'intégrité. Cependant, la faille est due au fait que ce code est calculé à partir d'une fonction linéaire : le CRC. Or, l'algorithme utilisé par le protocole Michael n'est pas linéaire et est donc invulnérable à cette faille.

1. La clé d'intégrité, de 128 bits, fait partie de la clé temporaire PTK ou GTK (voir paragraphes précédents).

Une faiblesse de Michael

Cependant, du fait des contraintes imposées par le matériel existant au moment de l'invention du protocole Michael, cet algorithme a été conçu pour être très rapide à exécuter, au détriment de la sécurité. Les concepteurs de Michael eux-mêmes ont calculé que le code MIC, malgré sa longueur de 64 bits, n'offrait en réalité qu'une sécurité d'environ 29 bits au maximum : autrement dit, si un pirate parvient à modifier un paquet et qu'il cherche à deviner le code MIC qu'il lui faut rajouter à ce nouveau paquet (sans connaître la clé d'intégrité bien sûr), alors il ne lui est pas nécessaire de tester les 2^{64} possibilités (environ 18 milliards de milliards), mais « seulement » environ 2^{29}, soit un demi-milliard.

Cela peut paraître beaucoup, mais en réalité, un paquet pirate sera accepté en moyenne en quelques jours seulement, s'il parvient à bombarder le point d'accès de paquets, à 20 Mb/s par exemple. Imaginez que ce paquet contienne une requête qui efface votre base de données ? Quitte à être légèrement paranoïaque, il ne faut pas accepter le risque qu'un seul paquet pirate puisse être injecté dans le réseau. Alors comment faire pour éliminer ce risque ?

Les contre-mesures

Conscients du problème de la faiblesse du code MIC, les concepteurs de TKIP ont conçu des « contre-mesures ». Si un paquet est reçu avec un ICV correct mais un code MIC erroné, alors l'AP renvoie un simple message d'erreur. Mais si un deuxième paquet est reçu avec un ICV correct mais un code MIC erroné dans les 60 secondes qui suivent, alors l'AP déclenche immédiatement les « contre-mesures » prévues par le protocole Michael : l'AP se bloque pendant 60 secondes, interdisant toute communication, les clés de cryptage temporaires sont toutes annulées et de nouvelles clés sont renégociées automatiquement, et enfin l'AP prévient généralement l'administrateur (par une alerte SNMP[1], ou un e-mail).

L'ICV sert à contrôler que le paquet n'a pas été altéré par des erreurs de transmission. Si le récepteur constate que l'ICV est erroné, alors il ignore silencieusement le paquet : le code MIC n'est même pas vérifié car l'on suppose que le paquet a simplement été mal transmis. L'ICV comporte 32 bits, donc la probabilité qu'un paquet erroné ait tout de même, par pur hasard, un ICV correct est d'environ une chance sur 4 milliards. C'est très peu... mais pas tout à fait négligeable : pour un réseau chargé, dans un environnement bruyant, il n'est pas impossible que cela se produise une fois par an. Les concepteurs de Michael auraient pu décider que les contre-mesures seraient déclenchées dès le premier paquet possédant un ICV correct et un code MIC erroné, mais ils ont préféré éviter le risque d'éventuelles fausses alertes. Ils ont donc choisi de ne déclencher les contre-mesures qu'au deuxième paquet suspect reçu en l'espace de 60 secondes : la probabilité qu'il s'agisse alors deux fois de suite d'erreurs

1. Le *Simple Network Management Protocol* (SNMP) est un protocole très apprécié pour la supervision d'un réseau. Pour un rappel sur les protocoles des réseaux IP, consultez l'annexe A sur le site *www.livrewifi.com*.

de transmission est tout simplement négligeable, et l'on peut affirmer avec certitude qu'un pirate est en train d'essayer d'injecter des paquets dans le réseau.

Les contre-mesures empêchent le pirate de faire des tentatives sans arrêt dans l'espoir de pouvoir injecter un paquet de temps en temps, car il lui faudrait en moyenne tester un demi-milliard de codes MIC avant d'en trouver un qui soit accepté... ce qui prendrait un demi-milliard de minutes (soit près de mille ans !), tout ça pour ne parvenir à injecter qu'un seul paquet dans le réseau. Bref, ce protocole Michael a bien fonctionné et tenu ses promesses pendant plusieurs années. Malheureusement, il a maintenant été cassé.

Le protocole Michael cassé fin 2008

Deux jeunes chercheurs allemands, Erik Tews et Martin Beck, ont découvert une faille dans le contrôle d'intégrité Michael. Ils ont même commencé à mettre au point l'outil *tkiptun*, téléchargeable gratuitement[1], qui vise à exploiter cette faille.

Voici le principe de cette attaque :

- le pirate commence par attendre qu'une requête ou réponse ARP soit émise sur le réseau : l'ARP est un protocole utilisé sur tous les réseaux IP lorsqu'une station veut connaître l'adresse MAC d'une station dont elle ne connaît que l'adresse IP[2]. Bien que les paquets soient cryptés par TKIP, on peut repérer facilement les paquets ARP car ils ont une taille caractéristique (51 octets en comptant l'IV, l'en-tête LLC, le paquet ARP proprement dit, le code MIC et l'ICV). Le contenu du paquet ARP est facile à deviner, pour l'essentiel. La plupart du temps, on ignore uniquement l'adresse IP recherchée (4 octets). Bien sûr, dans le message crypté, on ignore également le code MIC du protocole Michael (8 octets) et l'ICV (4 octets).
- Le pirate peut alors utiliser une attaque qui a fait ses preuves contre le WEP : l'attaque « *chop-chop* » (littéralement « découper-découper »). Le pirate essaie de deviner la valeur du dernier octet du message en clair, avant l'ICV (dans notre cas, il s'agit du dernier octet du code MIC). Il supprime ensuite l'octet correspondant dans le message crypté (le dernier octet crypté avant l'ICV crypté), et il calcule le nouvel ICV crypté pour ce paquet modifié. Il paraît très surprenant qu'il soit capable de calculer l'ICV crypté alors qu'il ne connaît pas les clés de cryptage, mais c'est rendu possible par le fait que l'ICV est un algorithme linéaire (voir le § 7.3.3) : lorsqu'on modifie un bit dans le message crypté, on peut savoir exactement quel bit changer dans l'ICV crypté pour que le paquet reste valide, sans qu'il soit nécessaire de connaître la clé de cryptage.
- Il envoie maintenant ce paquet crypté et tronqué d'un octet, dont l'ICV a été recalculé. S'il n'a pas correctement deviné le dernier octet du message en clair, alors il aura mal calculé l'ICV du paquet tronqué, et l'AP rejettera silencieusement ce paquet. Il lui suffit alors de recommencer la procédure en

1. http://www.aircrack-ng.org/doku.php?id=tkiptun-ng
2. Pour plus de détails sur le protocole ARP, voir l'annexe A disponible sur www.livrewifi.com.

essayant une autre valeur pour l'octet à deviner. Au bout de maximum 256 essais il tombera sur la bonne valeur : tout cela ne prendra que quelques instants. Le paquet aura alors un ICV correct, mais un code MIC incorrect. L'AP renverra donc un message d'erreur, comme cela est prévu par le protocole Michael : c'est une indication essentielle pour le pirate, car il sait maintenant qu'il avait bien deviné la valeur du dernier octet en clair, c'est-à-dire le dernier octet du code MIC en clair.

- Le pirate doit maintenant attendre 60 secondes avant de continuer, afin d'éviter que l'AP ne déclenche les contre-mesures. Une fois ce délai passé, il peut continuer l'attaque *chop-chop* pour deviner, par la même procédure, l'avant-dernier octet du message en clair. Il peut continuer ainsi pour chaque octet du message, en s'arrêtant une minute entre chaque octet deviné. Puisqu'il a 12 octets à deviner, il pourra les deviner en 12 minutes (plus quelques secondes) !
- Le pirate connaît alors l'intégralité du paquet en clair, dont le code MIC. À partir de cela, il peut inverser l'algorithme de calcul du code MIC pour trouver la clé d'intégrité ! En effet, le protocole de génération du code MIC a été conçu pour être simple et facile à calculer, mais pas pour être irréversible (on ne pensait pas qu'il pourrait être deviné facilement).
- Comme le pirate connaît maintenant le paquet en clair et sa version cryptée, il peut en déduire la séquence RC4 qui a été utilisée pour crypter ce paquet (hormis l'ICV). Il est donc maintenant capable de créer un paquet quelconque, d'une taille inférieure ou égale à 39 octets, il peut calculer le code MIC de ce paquet grâce à la clé d'intégrité qu'il a trouvée, et cela donne un message de maximum 47 octets. Il crypte ensuite le tout avec la séquence RC4 dont il dispose. Pour finir, même s'il ne connaît pas l'ICV en clair, il peut utiliser la propriété de linéarité de l'ICV pour calculer l'ICV crypté. Bref, il peut construire un nouveau paquet de son choix (mais de maximum 51 octets, ICV compris) : ce paquet est maintenant prêt à être injecté dans le réseau.
- Toutefois, il ne faut pas oublier les mesures anti-relecture : on ne peut pas émettre un paquet dont le TSC est inférieur au TSC_{max}. Or, puisqu'il s'est écoulé plus de 12 minutes depuis le début de l'attaque, le TSC_{max} a dû augmenter. Si le pirate veut tricher et augmenter la valeur du TSC de son paquet (qui correspond à l'IV, rappelons-le), alors il devra avoir un paquet crypté avec la clé RC4 correspondant à cet IV. Or, il ne connaît la séquence de cryptage que du paquet qu'il a décrypté, avec son TSC : il est donc condamné à n'utiliser que celui-là. Heureusement pour lui (et malheureusement pour la sécurité TKIP), il peut profiter du fait que le 802.11e utilise un TSC différent pour chaque classe de trafic. En changeant la classe du trafic de son paquet (un simple champ dans l'en-tête à modifier) le TSC de son paquet forgé sera comparé au TSC_{max} de la classe de trafic choisie. Son TSC pourra donc parfaitement être supérieur au TSC_{max} de cette classe : son paquet sera alors accepté ! Il peut recommencer sur chaque classe de trafic, et il pourra ainsi injecter jusqu'à 7 paquets de son choix, de 51 octets maximum, sur le réseau.

- Le pirate peut recommencer toute l'opération toutes les 12 minutes environ. Il peut donc injecter jusqu'à 7 paquets de son choix, d'une cinquantaine d'octets maximum, toutes les 12 minutes.

On voit que la faille est tout de même limitée : le pirate ne peut décrypter que de petits paquets ARP dont il n'ignorait finalement que deux octets, et il ne peut injecter réellement que quelques rares et petits paquets. Il ne possède pas les clés maîtresses (PMK et GMK) ou même temporaires, mise à part la clé d'intégrité, donc il ne peut pas décrypter l'ensemble du trafic. Néanmoins, cette attaque est vraisemblablement la première d'une série, et il est maintenant clair qu'il est temps de migrer vers l'AES.

9.3.5 Le mode mixte : WEP et WPA

Afin d'assurer une transition douce du WEP vers le WPA, il est possible de déployer, sur un même réseau, les deux solutions de sécurité (fig. 9.12). Pour cela, il faut que les AP gèrent ce « mode mixte » et bien sûr que celui-ci soit activé. Lorsqu'un AP en mode mixte reçoit un paquet envoyé par une station, il vérifie le type de cryptage utilisé en consultant le 6e bit du champ KeyID (voir § 9.3.2) qui se trouve dans tous les paquets WEP et TKIP. Si ce bit est égal à 0, il utilise le WEP, sinon il utilise le WPA. Bien entendu, il utilise la même méthode de cryptage pour l'envoi de paquets vers cette station.

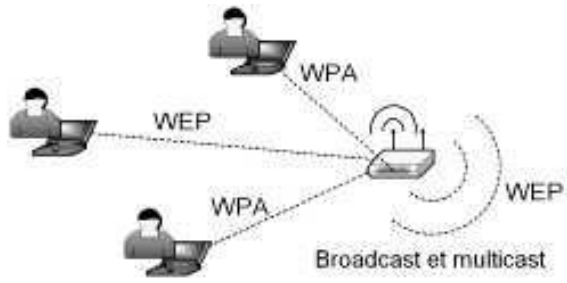


Figure 9.12 — Un réseau mixte WEP + WPA.

Un problème se pose avec le trafic de groupe (broadcast ou multicast) : faut-il le crypter avec TKIP ou avec le WEP ? Puisque les stations WEP ne comprennent rien à TKIP, on est obligé d'émettre ce trafic en le cryptant avec le WEP. Il faut donc s'assurer que toutes les stations WPA soient configurées également en mode mixte, afin qu'elles puissent décrypter le broadcast et le multicast. Si toutes les stations utilisent le WPA, il est recommandé de désactiver le mode mixte dans tous les AP et toutes les stations, afin de s'assurer que le WEP ne soit jamais utilisé.

> Le WEP possède de graves défauts et il faut essayer de passer le plus rapidement possible au WPA : le mode mixte ne doit donc être qu'une étape de transition et non l'état final de votre réseau.

Conclusion : malgré ses qualités, il existe une solution encore plus sûre que TKIP : si vous êtes particulièrement exigeant et que souhaitez avoir un niveau de sécurité encore plus élevé (notamment avec un mécanisme de contrôle d'intégrité plus puissant que Michael), le WPA2 avec AES est pour vous.

9.4 LA SOLUTION AES

9.4.1 Pourquoi AES ?

L'algorithme AES a été développé par deux Belges, Joan Daemen et Vincent Rijmen, dans les années 1990. Leur algorithme AES s'appelait alors « Rijndael », du nom de ses auteurs. L'*Advanced Encryption Standard* (AES), c'est-à-dire le « standard de cryptage avancé », est l'un des algorithmes de cryptage les plus puissants qui existent aujourd'hui : les meilleurs experts en sécurité se sont penchés dessus pendant plusieurs années sans lui trouver de faille exploitable. Le gouvernement des États-Unis a même décidé de l'adopter pour crypter ses propres communications, en remplacement de l'algorithme *Data Encryption Standard* (DES), déjà très réputé. Même la fameuse *National Security Agency* (NSA) crypte désormais ses documents « top secret » avec l'AES.

L'algorithme AES fait l'objet d'un véritable consensus de la part des instances les plus exigeantes en matière de sécurité.

En outre, l'AES est très performant : il n'utilise que des opérations simples telles que des additions, des décalages de bits ou encore l'opération XOR. Tout ceci en fait un algorithme extrêmement attrayant.

9.4.2 Le WPA/AES

WPA et WPA2

La sécurité et la performance de l'AES sont les deux raisons pour lesquelles le groupe de travail du 802.11i s'est tourné vers cet algorithme lorsqu'il cherchait une solution de sécurité plus sûre que le WEP. Ce groupe a alors développé une solution de sécurité complète reposant sur cet algorithme AES. Cette solution inclut :

- une authentification forte reposant sur le protocole 802.1x ;
- un mécanisme de distribution automatique des clés ;
- un contrôle d'intégrité puissant ;
- un mécanisme empêchant toute attaque de relecture.

Comme nous l'avons dit, il a malheureusement fallu beaucoup de temps à l'IEEE pour finaliser cette solution complète et c'est la raison pour laquelle le WPA a vu le jour. Celui-ci a copié l'authentification 802.1x et la distribution automatique de clés et il n'a conservé que l'algorithme TKIP, pour satisfaire les exigences des matériels WiFi existants.

En juin 2004, la norme 802.11i a enfin été ratifiée, introduisant le cryptage AES. Il est fréquent de ne pas distinguer le WPA et le WPA2 et de parler simplement de « WPA/TKIP » et de « WPA/AES » (vous l'aurez peut-être remarqué dans la figure 9.1).

Des stations WPA/TKIP et WPA/AES peuvent coexister sur un même réseau, pourvu que les AP gèrent ce nouveau « mode mixte ». Comme pour le mode mixte « WEP + WPA », le trafic de groupe dans un réseau mixte « TKIP + AES » est crypté avec l'algorithme le moins fort des deux, c'est-à-dire en l'occurrence le TKIP.

Le matériel WPA/AES

Le principal défaut du WPA/AES est qu'il requiert un matériel conçu pour le supporter.

C'est le cas de la grande majorité des produits récents, mais pas de tous : il faut donc faire attention aux produits que vous choisissez.

Le CCMP

L'AES, en soi, n'est qu'un algorithme de cryptage. Il est au WPA2 ce que le RC4 est au WEP : il en constitue le cœur, mais tout seul il ne sert à rien. Il faut donc un protocole qui définisse comment l'utiliser : pour le WPA/AES, ce protocole s'appelle le *CCM Protocol* (CCMP). Il définit précisément comment l'AES doit être utilisé pour crypter chaque paquet WiFi. Le CCMP spécifie également quel algorithme de contrôle d'intégrité doit être utilisé : il s'agit de l'algorithme CBC. Nous reviendrons sur le CCMP et le CBC plus loin.

Le tableau suivant résume les protocoles, les algorithmes de cryptage et les algorithmes de contrôle d'intégrité des solutions de sécurité WiFi :

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

Au fond, vous en savez maintenant bien assez pour pouvoir déployer le WPA/AES : il vous faut des AP et des stations qui le supportent et il faut sélectionner l'AES comme méthode de cryptage. Pour le reste tout est identique à l'architecture WPA, en particulier l'authentification 802.1x et la nécessité de déployer un serveur RADIUS (à moins d'utiliser une clé partagée PSK). Pour les plus curieux, nous allons maintenant détailler un peu le fonctionnement du WPA/AES.

9.4.3 Les modes de cryptage

Algorithmes par bloc ou par flux

Le protocole AES fait partie des algorithmes de cryptage « par bloc » : il prend un bloc de 128 bits et à l'aide d'une clé de cryptage (de 128, 192 ou 256 bits, au choix)[1] il fabrique un nouveau bloc de 128 bits, crypté. Ce nouveau bloc a un aspect tout à fait aléatoire et imprévisible, ce qui fait la force d'AES. Le protocole AES définit bien sûr comment récupérer le bloc original à partir du bloc crypté et de la clé de cryptage.

Le cryptage par bloc est différent de ce que nous avons vu avec l'algorithme RC4 : ce dernier génère un flux continu de bits pseudo-aléatoires que l'on utilise pour crypter les données bit par bit. Il s'agit d'un algorithme de cryptage « par flux ».

Un avantage des algorithmes de cryptage par bloc est qu'on ne peut pas savoir à quel bit crypté correspond tel bit non crypté. En d'autres termes, si l'on modifie un seul bit du message non crypté, alors le message crypté sera peut-être entièrement différent (ou en tout cas, au moins un bloc sera différent). Avec le RC4, un danger est que le pirate sait exactement où se trouve le bit crypté correspondant au bit en clair qu'il veut modifier. S'il sait comment tromper le système de contrôle d'intégrité (et ce n'est pas difficile avec le WEP, par exemple), alors il peut modifier le message à l'endroit de son choix. Cela ne lui permet toutefois pas de deviner ce que sa modification donnera, une fois décryptée.

Qu'est-ce qu'un « mode » ?

La stratégie d'utilisation d'un algorithme de cryptage s'appelle le « mode ». Par exemple, le mode le plus simple qui soit pour un algorithme par bloc consiste à découper le message à crypter en blocs de la bonne taille et de les crypter un à un (fig. 9.13). Ce mode s'appelle l'*Electronic Code Book* (ECB). Bien entendu, on peut utiliser ECB avec tout algorithme de cryptage par bloc. Lorsqu'on l'utilise avec AES, on le note : ECB-AES. Le mode ECB possède plusieurs défauts :

- le message à crypter doit obligatoirement avoir une longueur qui soit un multiple de la taille des blocs ;
- puisque tous les blocs sont cryptés avec la même clé, si deux blocs sont identiques, alors ils produisent le même bloc crypté.

Ce deuxième point est le plus gênant. En effet, admettons que vous souhaitiez envoyer un message dont tous les blocs soient identiques, par exemple « 123412341234... » : le message crypté sera lui-même composé d'une répétition de blocs identiques. Ce n'est pas pour autant que le pirate pourra décrypter votre message, mais il aura déjà appris quelque chose au sujet des informations que vous envoyez... et c'est ce que l'on veut éviter.

Ceci nous permet de voir l'importance du mode : même avec l'algorithme de cryptage le plus puissant qui soit, un mauvais mode peut tout gâcher. C'est ce qui s'est

1. L'algorithme Rijndael est identique à l'AES, mais il autorise des blocs et des clés de 128, 160, 192, 224 ou 256 bits, au choix. Dans la conception d'AES, il a été décidé que cette souplesse était inutile.

passé avec le WEP : l'algorithme RC4 est très bon, mais l'utilisation qui en a été faite ne l'est pas. Pour cette raison, WPA/AES utilise un mode bien plus sûr que le mode ECB.

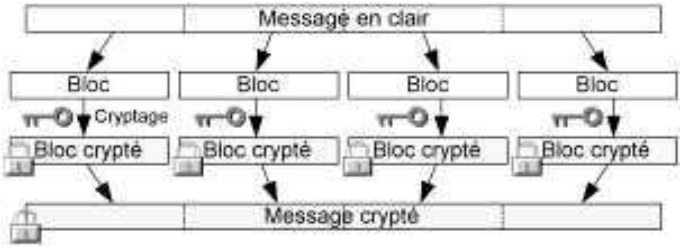


Figure 9.13 — Le mode *Electronic Code Book* (ECB).

Le Counter-Mode

Un mode très apprécié pour les algorithmes par bloc est le *Counter-Mode* (CM), c'est-à-dire le « mode compteur ». Il est utilisé depuis plus de vingt ans et est considéré comme très sûr. Son principe est cependant légèrement plus complexe que celui d'ECB (fig. 9.14) :

- un compteur est incrémenté sans arrêt ;
- ce compteur lui-même est crypté avec l'algorithme de cryptage par bloc choisi (en utilisant la clé de cryptage bien sûr) ;
- ceci produit un flux infini de bits pseudo-aléatoires, un peu comme RC4. Ce flux est simplement combiné avec le message, grâce à l'opération XOR.

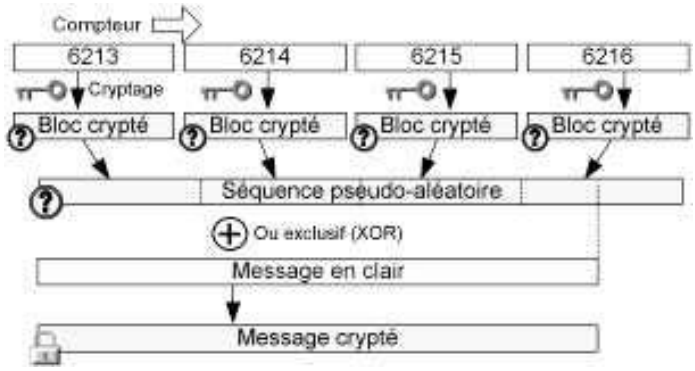


Figure 9.14 — Le Counter-Mode (mode compteur)

Avec le Counter-Mode, un algorithme par bloc est transformé finalement en un algorithme par flux.

Ceci apporte quelques avantages intéressants : d'abord la taille du message à crypter n'a plus besoin d'être un multiple de la taille du bloc. En outre, l'opération de décryptage est strictement identique à l'opération de cryptage, ce qui permet de ne pas avoir à mettre en œuvre la fonction de décryptage de l'algorithme par bloc utilisé. Enfin, le problème de la répétition des blocs n'existe plus car le compteur change pour chaque bloc de bits pseudo-aléatoires produit.

Malheureusement, le Counter-Mode réintroduit le problème que nous avons mentionné plus haut : puisque l'on a maintenant un algorithme par flux, les bits sont cryptés un à un et la position d'un bit crypté correspond à celle de ce bit non crypté. Il faut donc que l'algorithme de contrôle d'intégrité soit très sûr. Par bonheur, avec le WPA2, c'est le cas.

Le CCM

Le WPA/AES repose quant à lui sur un mode inventé par le groupe de travail 802.11i : ce mode porte le nom un peu obscur de *Counter-Mode + CBC-MAC* (CCM). Comme ce nom l'indique, CCM repose sur le Counter-Mode pour le cryptage. En outre, l'algorithme de contrôle d'intégrité CBC-MAC est utilisé.

Le code CBC

CBC-MAC signifie *Cipher Block Chaining-Message Authentication Code*, ce qui peut se traduire par « code d'intégrité de message calculé par le chaînage d'un algorithme de cryptage par bloc ». Oui, c'est un peu plus long en français ! Notez que dans le contexte de la sécurité, l'abréviation « MAC » n'a absolument rien à voir avec la *couche* MAC dont nous avons parlé jusqu'à présent. Pour éviter toute confusion, nous parlerons donc simplement de code CBC. Voyons comment ce code est calculé (fig. 9.15) :

- le premier bloc du message est crypté avec AES[1] ;
- ce bloc crypté est combiné avec le deuxième bloc non crypté, grâce à l'opération XOR ;
- le résultat est lui-même crypté avec AES et ainsi de suite, bloc par bloc.

Le code CBC qui résulte de ce calcul a la longueur d'un bloc. Sa valeur est complètement imprévisible : si un seul bit du message change, le code CBC change complètement. Il s'agit donc d'un excellent code de contrôle d'intégrité. Son principal défaut est qu'il est gourmand en puissance de calcul, contrairement à Michael, par exemple. En outre, il ne peut fonctionner que si le message a une longueur égale à un multiple de la taille des blocs. Le protocole CCMP utilisé par WPA/AES résout ce problème en complétant le message avec des zéros jusqu'à obtenir une taille adéquate (en anglais, cela s'appelle du *padding*) : les zéros ne sont pas rajoutés au message à envoyer ; ils sont seulement utilisés pour le calcul du code CBC.

1. En fait, le mode CCM est conçu pour fonctionner avec tout algorithme de cryptage par bloc.

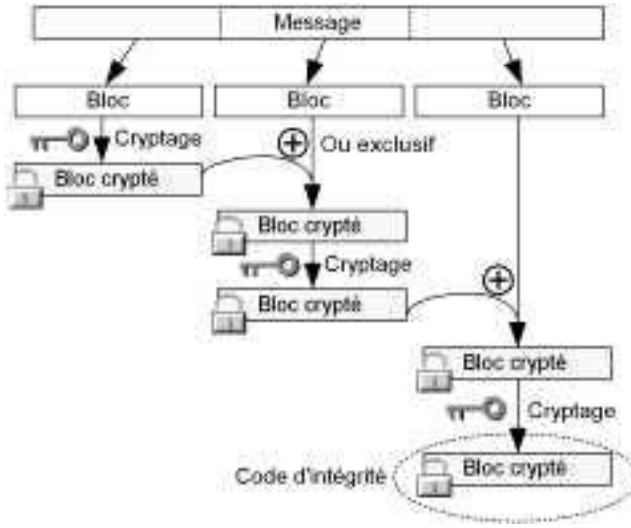


Figure 9.15 — Le code d'intégrité CBC.

Les ajouts de CCM

Le mode CCM repose sur le Counter-Mode pour le cryptage et le code CBC pour le contrôle d'intégrité. La même clé est utilisée pour le cryptage est pour le calcul du code CBC. Le CCM rajoute en outre un élément essentiel : il utilise un *nonce* (un numéro unique) de 48 bits pour crypter et calculer le CBC de chaque message, afin que deux messages identiques envoyés avec la même clé ne donnent jamais le même résultat. Ce *nonce* est en fait séquentiel et il est également utilisé pour éviter les attaques de relectures. On l'appelle le numéro de paquet (*Packet Number*, PN) et il a le même rôle que le numéro de séquence TSC de TKIP.

Enfin, le mode CCM rajoute également une fonctionnalité intéressante : le code CBC peut être calculé sur le message crypté *plus* des éléments non cryptés. Cela peut permettre au récepteur de s'assurer qu'un champ non crypté, comme l'adresse MAC source d'un paquet par exemple, n'a pas été modifié par un pirate.

9.4.4 Le CCMP

L'en-tête CCMP

Bien que le mode CCM ait été conçu par le groupe de travail du 802.11i, il peut être utilisé dans n'importe quel autre contexte. C'est pourquoi le 802.11i définit également le CCM *Protocol* (CCMP), dont le rôle est de préciser exactement comment le CCM doit être utilisé dans le contexte du WiFi.

Pour détailler le CCMP, il faut rappeler brièvement comment un paquet à envoyer est traité par la couche MAC :

- le paquet fourni à la couche MAC par les couches réseau supérieures s'appelle le MSDU ;

- la couche MAC commence éventuellement par fragmenter le MSDU en plusieurs paquets appelés les MPDU ;
- chaque MPDU est composé d'un en-tête MAC et des données.

Dans le cas de WEP, un en-tête WEP est rajouté entre l'en-tête MAC et les données : il contient l'IV et l'index de la clé WEP. Dans le cas de TKIP, un en-tête TKIP est également rajouté : il est composé de l'IV étendu et de l'index de la clé WEP. Dans le cas de CCMP, un en-tête est également rajouté entre l'en-tête MAC et les données : il a une structure semblable à celle de l'en-tête TKIP et contient le numéro de paquet (PN) de 48 bits utilisé par CCM, ainsi que l'index de la clé temporaire (PTK ou GTK) utilisée pour le cryptage (utile uniquement pour le trafic de groupe, comme pour TKIP). Voici la structure de l'en-tête CCMP :

PN0	PN1	Rsv	ID	PN2	PN3	PN4	PN5
1 octet	1 octet	1 octet	1 octet	1 octet	1 octet	1 octet	1 octet

On voit que les 48 bits (6 octets) du PN, de PN0 à PN5, ne sont pas contigus. Le but est de conserver une structure similaire à celle de l'en-tête TKIP et WEP. On retrouve notamment le champ ID du WEP et de TKIP. Le troisième octet de l'en-tête CCMP est réservé pour un usage futur.

Cet en-tête CCMP est donc rajouté entre l'en-tête MAC et les données cryptées par le Counter-Mode/AES. Seule la moitié du code CBC est conservée pour former le code d'intégrité (8 octets, c'est déjà bien suffisant). Ce code, appelé le *Message Integrity Code* (MIC), est rajouté à la fin des données à crypter. Voici donc la structure d'un paquet crypté avec le WPA/AES :

En-tête MAC	En-tête CCMP	Données cryptées	MIC crypté	CRC
30 octets	8 octets	0 à 2 296 octets	8 octets	4 octets

Des en-têtes protégés

Une originalité de CCMP est le fait que l'en-tête MAC et l'en-tête CCMP sont utilisés pour calculer le code CBC (qui donne le code MIC), en plus des données. L'intérêt, comme nous l'avons dit, est de protéger ces champs contre des modifications d'un pirate. Ni le WEP ni TKIP n'offraient cette protection. Cela signifiait qu'un pirate pouvait facilement modifier un paquet en changeant par exemple l'adresse MAC source et en la remplaçant par la sienne pour que la réponse lui soit envoyée.

Cependant, les en-têtes ne sont pas utilisés tels quels pour calculer le MIC. En effet, certains des champs des en-têtes sont susceptibles d'être modifiés, de façon tout à fait légitime, par l'adaptateur réseau. C'est le cas notamment si une stratégie de qualité de service est mise en œuvre et que la priorité du paquet peut être modifiée en fonction de l'état du réseau. Ces champs modifiables sont exclus du calcul du MIC : pour cela,

ils sont remplacés par des zéros. Bien sûr, ce remplacement est uniquement réalisé pour le calcul du MIC : les champs effectivement envoyés ne sont pas réellement remplacés par des zéros. Une fois calculé, le MIC est rajouté à la fin des données et il est crypté avec elles (fig. 9.16).

> Avec le CCMP, le code d'intégrité MIC est calculé sur l'ensemble du message plus l'en-tête CCMP et MAC, hormis les champs modifiables. Contrairement au WEP et à TKIP, les en-têtes sont donc protégés.

Le calcul du code d'intégrité spécifié par CCM fait intervenir, comme nous l'avons dit, le PN, de sorte que deux messages identiques n'aboutissent jamais deux fois au même MIC. En outre, l'adresse MAC de l'émetteur est utilisée pour éviter que deux stations utilisant la même clé et le même PN ne génèrent le même code d'intégrité pour un même message. On retrouve donc les mêmes principes que pour TKIP.

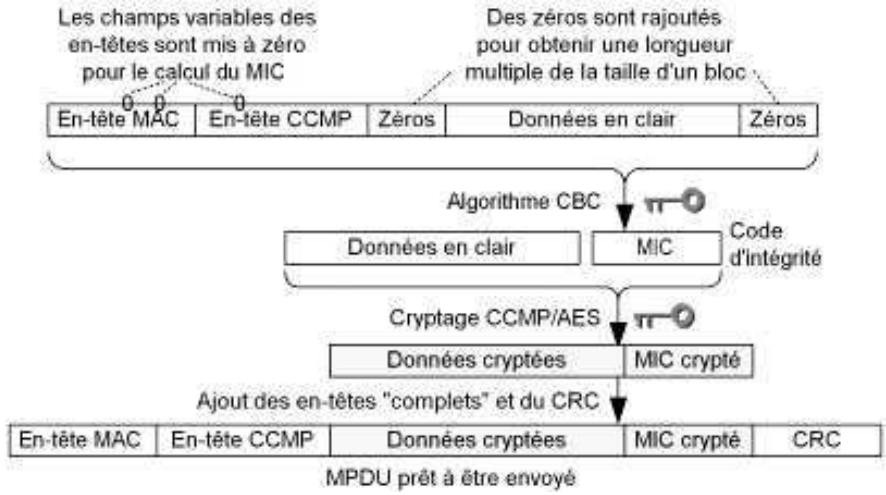


Figure 9.16 — Le calcul d'intégrité de CCMP.

Le cryptage

Le cryptage du CCMP est réalisé avec le CCM/AES (fig. 9.17). L'algorithme de cryptage est le *Counter-Mode*/AES, mais le compteur sur lequel repose cet algorithme contient le PN et l'adresse MAC de l'émetteur, plus une partie qui augmente pour chaque bloc crypté, selon le principe du *Counter-Mode*. Comme pour le calcul du MIC, ceci permet de garantir que deux stations possédant la même clé, le même PN et envoyant le même message n'obtiendront jamais deux fois le même résultat.

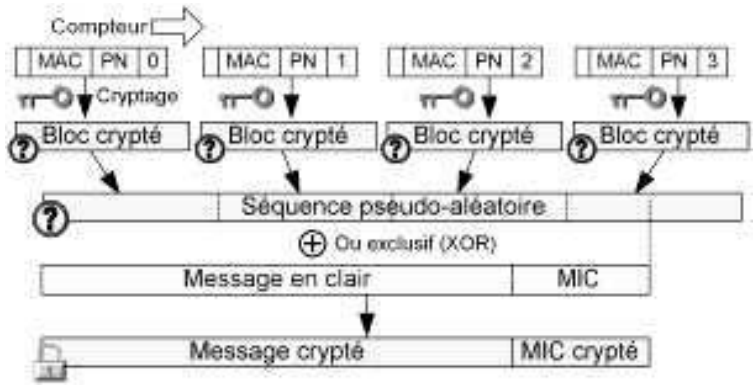


Figure 9.17 — Le cryptage de CCMP.

Voici le format du compteur utilisé pour le cryptage *Counter-Mode*/AES :

Options	Priorité	Adresse MAC	PN	Compteur
1 octet	1 octet	6 octets	6 octets	2 octets

Les deux premiers champs correspondent à des champs des en-têtes. L'adresse MAC est celle de l'émetteur.

Résumé

Le *nec plus ultra* de la sécurité WiFi est offert par la norme IEEE 802.11i, ratifiée en juin 2004. Un sous-ensemble de cette norme a été publié deux ans auparavant par la WiFi Alliance sous le nom de WPA. Alors que le 802.11i autorise deux types de cryptages, le TKIP et l'AES, le WPA ne gère quant à lui que le TKIP. En outre, le WPA ne fonctionne théoriquement pas en mode Ad Hoc, contrairement au 802.11i. La WiFi Alliance a commencé la certification WPA2 en septembre 2004 pour les produits compatibles avec toute la norme 802.11i.

Pour utiliser le WPA2 sur AES, il est nécessaire de disposer de matériel récent, capable de le supporter. En revanche, une simple mise à jour de *firmware* est souvent suffisante pour rendre un ancien matériel WiFi compatible avec le TKIP.

Pour déployer le WPA ou le WPA2, le plus simple consiste à saisir une *passphrase* identique dans chaque équipement. C'est la méthode « PSK », également appelée « WPA Personal ». Cette méthode est recommandée pour les particuliers (ou les très petites entreprises) car elle est très simple à mettre en œuvre. Cependant, elle n'offre pas le meilleur niveau de sécurité et est trop lourde à gérer pour les grands réseaux. Il est absolument impératif de choisir une *passphrase* longue et complexe, et de la changer régulièrement.

En entreprise, il est fortement recommandé de mettre en place une architecture 802.1x, comme nous l'avons décrit au chapitre précédent. On parle d'architecture WPA Enterprise. Cela implique de choisir une méthode d'authentification EAP, telle que le PEAP/MD5 par exemple, puis d'installer et de configurer un serveur RADIUS gérant la méthode choisie. Il faut également installer et configurer un logiciel de connexion WPA compatible avec la méthode EAP choisie, sur le poste de chaque utilisateur. Il faut bien sûr s'assurer aussi que tous les AP soient bien compatibles WPA Enterprise et les configurer pour qu'ils fassent appel au bon serveur RADIUS.

Le WPA et le WPA2 permettent notamment :

– la distribution automatique d'une clé maîtresse (PMK) au cours de l'authentification. Pour cela, une méthode EAP génératrice de clé doit être utilisée : les méthodes reposant sur des tunnels font l'affaire et sont recommandées ;

– la négociation automatique de clés temporaires pour le cryptage et le contrôle d'intégrité. Cette négociation a lieu entre le client et l'AP, à partir de la clé PMK qui est ainsi protégée ;

– un cryptage puissant, mis en œuvre par le protocole TKIP (basé sur RC4), ou par le protocole CCMP (basé sur AES) ;

– un contrôle d'intégrité reposant sur le protocole Michael dans le cas de TKIP/RC4 (malheureusement, ce protocole a été cassé fin 2008, comme nous l'avons vu) et sur l'algorithme CBC dans le cas de CCMP/AES ;

– des cryptages différents dans un même réseau : c'est le « mode mixte » ;

– un compteur incrémenté à chaque paquet pour contrer les attaques de relectures.

La solution TKIP était une solution de transition vers l'AES. Son mécanisme de contrôle d'intégrité Michael ayant été cassé, il est désormais fortement conseillé de passer effectivement à l'AES. Le WPA2/AES est une solution de sécurité unanimement considérée comme extrêmement robuste : elle est tout à fait apte à assurer la sécurité d'un réseau sans fil d'entreprise.

10

Le RADIUS

Objectif

Dans ce dernier chapitre, nous allons présenter le protocole et les serveurs RADIUS, qui servent avant tout à identifier les utilisateurs d'un service. Ce protocole ne fait pas partie de la norme 802.11 et il peut être utilisé dans bien d'autres contextes que les réseaux sans fil. Cependant, il est tout à fait central lorsque l'on met en œuvre une architecture 802.1x, ce qui est généralement le cas dans un réseau WiFi d'entreprise protégé par les nouvelles solutions de sécurité, le WPA ou le WPA2[1].

Au cours de ce chapitre, nous commencerons par étudier les trois rôles d'un serveur RADIUS : l'authentification des utilisateurs, la définition de leurs autorisations et la comptabilisation de leurs connexions. Ensuite, nous présenterons le protocole en précisant les éléments nécessaires à la configuration d'un serveur RADIUS et nous finirons par une présentation détaillée de la sécurité de l'architecture RADIUS.

10.1 LES FONCTIONS DU SERVEUR RADIUS

10.1.1 L'authentification

Un scénario de connexion

Le *Remote Authentication Dial In User Service* (RADIUS) est un protocole défini par l'IETF (voir le chapitre 8) dans la RFC 2865. De nombreuses RFC viennent étendre ce protocole, qui a été conçu pour être très ouvert. Son nom peut être traduit par « service d'authentification à distance pour des connexions d'utilisateurs ». En d'autres termes,

1. À moins d'utiliser une clé partagée (PSK). Voir le chapitre 9.

sa fonction première est de centraliser l'authentification des utilisateurs qui cherchent à se connecter à un réseau ou à un service quelconque. Le scénario élémentaire est le suivant (fig. 10.1) :

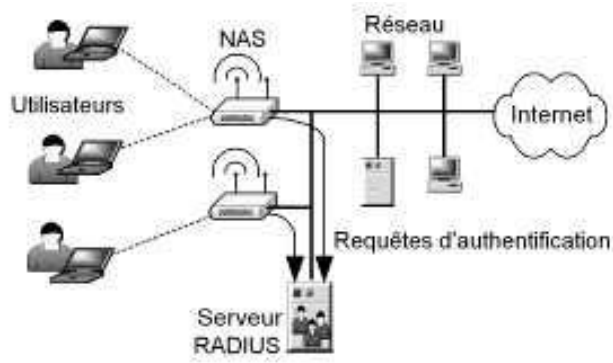


Figure 10.1 — L'architecture RADIUS

- Un utilisateur souhaite accéder à un réseau et pour cela il se connecte à un équipement qui contrôle son accès : cet équipement s'appelle le *Network Access Server* (NAS), c'est-à-dire le « serveur d'accès au réseau ». *Attention* : dans le contexte du protocole RADIUS, le NAS est souvent appelé le « client », ce qui peut réellement prêter à confusion. Lorsque vous configurez un serveur RADIUS, faites attention à ne pas confondre client et utilisateur.
- L'utilisateur fournit son identité au NAS, d'une manière ou d'une autre : le protocole utilisé pour cela n'est pas spécifié par RADIUS ; cela peut être n'importe quel protocole.
- En utilisant le protocole RADIUS, le NAS communique alors avec le serveur[1] afin de valider l'identité de l'utilisateur. Si le serveur RADIUS authentifie bien l'utilisateur, il en informe le NAS et celui-ci laisse désormais l'utilisateur accéder au réseau.

Plusieurs NAS peuvent être configurés pour faire appel au même serveur RADIUS et lui déléguer le travail d'authentification des utilisateurs. De cette façon, il n'est pas nécessaire à chaque NAS de posséder une copie de la liste des utilisateurs : celle-ci est centralisée par le serveur RADIUS.

Dans le cas d'un réseau WiFi, chaque AP peut jouer le rôle de NAS. C'est le cas lorsque l'on utilise l'architecture 802.1x.

1. Il existe de nombreux serveurs RADIUS sur le marché. Quelques-uns des plus répandus sont présentés dans le chapitre 8, au paragraphe 8.2.1. Ce chapitre a pour but de présenter le protocole RADIUS, ses concepts et sa sécurité et non de se substituer à la documentation de votre serveur RADIUS particulier.

Des méthodes d'authentification variées

Selon les différents serveurs RADIUS qui existent, les méthodes d'authentification prises en charge peuvent varier. Tous sont capables de vérifier l'identité d'un utilisateur grâce à un mot de passe, selon les protocoles PAP ou CHAP (voir le chapitre 8, paragraphe 8.1.3) et la grande majorité gère également les protocoles MS-CHAP ou MS-CHAP-v2. En outre, la plupart des serveurs RADIUS savent identifier les utilisateurs avec quelques-unes des méthodes EAP, telles que EAP/MD5 ou PEAP/MS-CHAP-v2. C'est le cas qui nous intéresse avec le WiFi : nous y reviendrons plus loin.

> La richesse des méthodes d'authentification d'un serveur RADIUS constitue l'un des critères de choix les plus importants.

Les connecteurs

Pour valider les mots de passe (ou toute autre preuve d'identité), certains serveurs RADIUS consultent simplement un fichier contenant la liste des utilisateurs et de leurs mots de passe (fig. 10.2). D'autres sont capables de lire ces informations dans une base de données relationnelle, comme MySQL ou Oracle. Certains peuvent consulter un serveur LDAP ou un contrôleur de domaine de Windows NT. Certains serveurs RADIUS vous laissent même la possibilité de programmer vous-même votre propre « connecteur » : vous pouvez ainsi relier le serveur RADIUS au système de votre choix, selon la méthode que vous préférez.

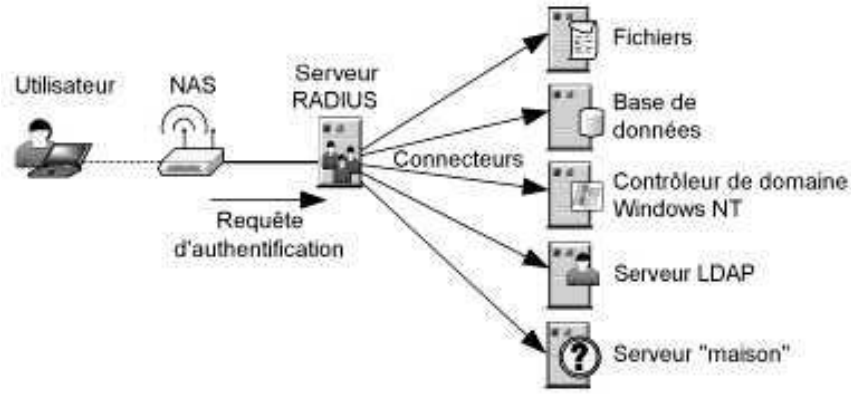


Figure 10.2 — Les connecteurs des serveurs RADIUS.

La plupart des sociétés possèdent déjà un serveur destiné à identifier les utilisateurs, par exemple un contrôleur de domaine Windows ou un serveur Kerberos. Lorsqu'elles apprennent que pour déployer une solution WiFi sécurisée, il est nécessaire de mettre en place un serveur RADIUS pour gérer l'authentification des utilisateurs, elles sont naturellement réticentes. Il faut donc insister sur ce point.

Il est tout à fait possible de conserver son serveur d'authentification existant et de configurer le serveur RADIUS pour qu'il fasse appel à lui, grâce à un « connecteur ».

Il faut bien sûr choisir un serveur RADIUS qui possède le connecteur adapté et le configurer correctement.

Les serveurs proxy

Les serveurs RADIUS peuvent également être configurés pour rediriger les requêtes de certains utilisateurs vers d'autres serveurs RADIUS (fig. 10.3). Lorsqu'un serveur redirige une requête, on dit qu'il est le *proxy*, c'est-à-dire le relais. Ce mécanisme peut être très utile, par exemple si une entreprise possède plusieurs bureaux : mettons un à Lyon et un à Rennes. Chaque bureau gère ses propres utilisateurs et possède son propre serveur RADIUS. Un jour, un employé du bureau de Lyon se rend à Rennes et cherche à se connecter au réseau. À ce moment, le NAS lui demande son identifiant et son mot de passe. Il saisit alors son identifiant, combiné à ce qu'on appelle le *realm* (le royaume). En général il saisira quelque chose comme « alain@lyon », mais selon la configuration du système, le format peut varier. De cette façon, lorsque le serveur RADIUS de Rennes recevra la requête d'authentification, il saura qu'il faut la rediriger vers le serveur RADIUS du bureau de Lyon. Celui-ci pourra valider le mot de passe de l'employé et sa réponse sera relayée par le serveur RADIUS de Rennes jusqu'au NAS, qui laissera alors l'employé accéder au réseau de Rennes.

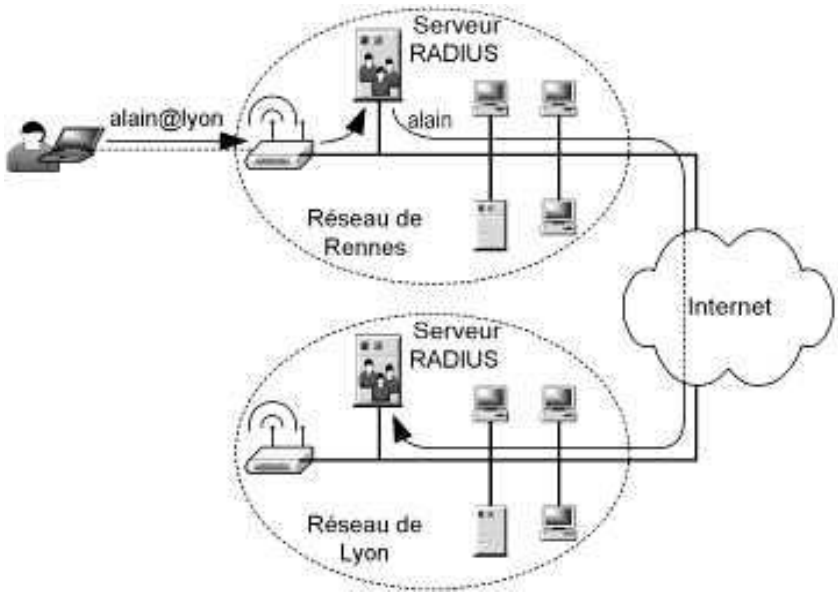


Figure 10.3 — Le proxy RADIUS.

Le proxy RADIUS est également au centre des accords d'itinérance (*roaming*) entre opérateurs : lorsqu'un abonné d'un opérateur *A* se connecte au réseau de *B*, le

NAS auquel il se connecte lui demande de s'authentifier, puis contacte naturellement le serveur RADIUS de *B*. Ce dernier, détectant (d'après son identifiant) que l'utilisateur est un abonné de l'opérateur *A*, se contente de rediriger la requête au serveur RADIUS de *A*. Ceci explique pourquoi votre identifiant de connexion ADSL ressemble à *identifiant@opérateur*, ou encore un format du type *opérateur/identifiant* : par exemple, *fti/dupond*, pour un abonné d'Orange.

10.1.2 L'autorisation

Un paramétrage fin et dynamique

Le rôle du protocole RADIUS ne s'arrête pas à la simple authentification. En effet, lorsque le serveur informe le NAS que l'utilisateur est bien authentifié, il peut en profiter pour fournir au NAS toutes sortes de paramètres (on parle plutôt « d'attributs ») utiles pour configurer la connexion de cet utilisateur. Par exemple, il peut indiquer au NAS que cet utilisateur ne doit pas accéder à telle ou telle partie du réseau, qu'il doit être déconnecté au bout de 30 minutes ou encore qu'il faut lui couper sa connexion s'il télécharge plus de 200 Mo.

> Le serveur RADIUS peut finement gérer les autorisations des utilisateurs, en transmettant au NAS des attributs variés. Pour cela, il suffit de configurer le serveur RADIUS en précisant les attributs à renvoyer pour chaque utilisateur ou groupe d'utilisateurs.

Les attributs standards

Quelques attributs possibles pour régler les autorisations des utilisateurs sont définis dans la RFC 2865 : par exemple, l'attribut *Session-Timeout* est défini comme un entier de 32 bits qui représente le nombre de secondes maximum que devra durer la session de l'utilisateur : une fois ce délai écoulé, le NAS doit déconnecter l'utilisateur, de force. L'attribut *Idle-Timeout* est également un entier de 32 bits : son rôle est d'indiquer au NAS au bout de combien de secondes d'inactivité l'utilisateur doit être déconnecté.

La RFC 2865 définit encore une vingtaine d'autres attributs, dont la plupart ne sont utiles que dans le contexte PPP (voir le chapitre 8, paragraphe 8.1.2) et non dans le contexte du WiFi. D'autres RFC définissent des attributs supplémentaires et la liste ne fait qu'augmenter, d'année en année.

Attributs spécifiques à des constructeurs

Par ailleurs, le protocole RADIUS autorise l'échange d'attributs spécifiques à certains constructeurs : on parle d'attributs *Vendor-Specific*. Par exemple, le constructeur Colubris Networks, qui fabrique des points d'accès (AP) WiFi, a défini un attribut appelé *Colubris-AVPair* qui peut transporter divers paramètres spécifiques à ses AP. Le serveur RADIUS peut être configuré pour utiliser l'attribut *Colubris-AVPair* lorsque l'utilisateur se connecte par le biais d'un AP de ce constructeur.

Par exemple, un utilisateur pourrait avoir la configuration suivante :

```
Idle-Timeout = 3600
Colubris-AVPair = access-list=acl,DENY,all,10.0.0.0/16,all
Colubris-AVPair = access-list=acl,DENY,all,10.1.0.0/16,all
Colubris-AVPair = user-access-list=acl
```

Le premier attribut précise que l'utilisateur doit être déconnecté au bout d'une heure d'inactivité. Le deuxième et le troisième attribut définissent une liste d'accès, appelée arbitrairement « acl » : l'utilisateur ne pourra pas (DENY) accéder aux sous-réseaux 10.0.0.0/16 et 10.1.0.0/16, quels que soient les protocoles (all) et quel que soit le port (all). Le dernier attribut active la liste d'accès « acl ».

Les attributs spécifiques à des constructeurs sont extrêmement variés et souvent très utiles. Certains permettent, par exemple, d'associer un utilisateur à un réseau virtuel (VLAN) donné, en fonction de ses droits d'accès. D'autres indiquent vers quel serveur SMTP doivent être redirigés tous les e-mails envoyés par un utilisateur (voir la transparence SMTP, au chapitre 4). Et ainsi de suite.

Toutefois, comme leur nom l'indique, ils ne fonctionnent que pour un constructeur donné[1]. Il faut donc les utiliser avec précaution et parcimonie, surtout dans un environnement où les NAS sont hétérogènes.

10.1.3 La comptabilisation

Début de session

La troisième et dernière fonction d'un serveur RADIUS, définie dans la RFC 2866, est de comptabiliser les connexions des utilisateurs. Voici comment cela fonctionne : dès qu'un NAS a reçu du serveur la confirmation de l'authentification d'un utilisateur (accompagnée d'attributs d'autorisation), il envoie une requête au serveur indiquant le début de la session de l'utilisateur. Cette requête comporte de nombreuses informations concernant la session et notamment :

- l'identifiant de session (*Acct-Session-Id*) ;
- l'identifiant de l'utilisateur (*User-Name*) ;
- l'identifiant du NAS (*NAS-Identifier*) ;
- l'adresse (MAC, en général) de l'utilisateur (*Calling-Station-Id*) ;
- l'adresse du NAS (*Called-Station-Id*).

Le serveur enregistre cette information (ainsi que l'heure exacte).

1. Quelques attributs *Vendor-Specific* font l'objet d'un consensus et sont utilisés par plusieurs constructeurs. Si l'engouement pour un attribut est important, il finit par être intégré dans une RFC.

Fin de session

Lorsque l'utilisateur met fin à sa session, ou que le NAS le déconnecte (ou encore si la connexion est coupée), le NAS envoie une requête au serveur RADIUS afin de lui indiquer que la session est terminée. Cette requête comporte à nouveau de nombreuses informations au sujet de la session, parmi lesquelles on trouve en général :

- la durée totale de la session, en secondes (*Acct-Session-Time*) ;
- le volume total de données téléchargées pendant la session, en nombre d'octets (*Acct-Input-Octets*) ou en nombre de paquets (*Acct-Input-Packets*) ;
- le volume total de données envoyées pendant la session, en nombre d'octets (*Acct-Output-Octets*) ou en nombre de paquets (*Acct-Output-Packets*) ;
- la cause de la fin de la session (*Acct-Terminate-Cause*), par exemple la demande de l'utilisateur (*User Request*), la perte du signal (*Lost Carrier*), la fin de la session (*Session Timeout*) ou encore une inactivité trop longue (*Idle Timeout*) ;
- plus tous les attributs précédents : *Acct-Session-Id*, *User-Name*, *NAS-Identifier*, *Calling-Station-Id*, *Called-Station-Id*...

Le NAS peut également être configuré pour envoyer des requêtes à intervalles réguliers, pendant la session de l'utilisateur, afin d'indiquer l'état de la session. Cette requête s'appelle un *Interim-Update*, c'est-à-dire une « mise à jour intermédiaire ». Elle peut contenir toutes les informations précédentes.

Comptabilisation et administration

Grâce à la comptabilisation très précise des connexions, il est possible de conserver une trace détaillée de toutes les connexions des utilisateurs. Si l'on possède un bon outil d'analyse des historiques de connexion, il est possible de bien contrôler l'accès au réseau.

On peut ainsi voir, par exemple, quels sont les NAS les plus utilisés, quels sont les utilisateurs qui téléchargent le plus de données ou encore la durée moyenne d'une session (fig. 10.4). On peut également détecter des tentatives d'intrusion ou se rendre compte de problèmes de connexion fréquents (*Lost Carrier*). Bref, c'est un outil très précieux pour l'administrateur réseau.

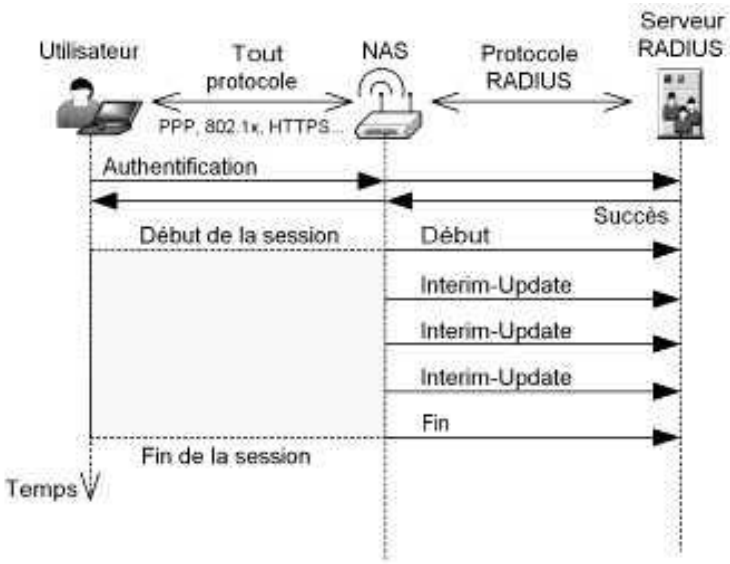


Figure 10.4 — La comptabilisation des connexions.

Comptabilisation et facturation

En outre, la comptabilisation des connexions, à la seconde et à l'octet près, permet de facturer précisément le service offert ! Bien sûr, ceci ne s'applique pas aux employés d'une entreprise, mais est mis à profit par les fournisseurs d'accès à Internet (FAI), avec ou sans fil. Dès sa conception, le protocole RADIUS a rapidement connu le succès dans le monde des FAI pour gérer les utilisateurs, leurs droits et la comptabilisation de leurs connexions en vue de la facturation.

C'est ainsi que les *Broadband Access Server* (BAS), qui contrôlent l'accès à Internet pour les abonnés ADSL, font en général appel à un serveur RADIUS. De même, les points de présence (PoP) d'un opérateur[1], pour les connexions à Internet *via* un simple modem téléphonique au travers du réseau téléphonique commuté (RTC), se connectent eux-mêmes à un serveur RADIUS pour identifier les utilisateurs, gérer leurs droits et comptabiliser leurs connexions. Les contrôleurs d'accès des *hotspot-in-a-box* (voir le chapitre 4), font très souvent appel à un serveur RADIUS.

Le serveur RADIUS est parfois appelé le « serveur AAA ». Ce sont les initiales, en anglais, des trois fonctions principales du serveur RADIUS, que nous venons de voir : *Authentication*, *Authorization*, *Accounting*, c'est-à-dire l'authentification, l'autorisation et la comptabilisation. Notons qu'il existe d'autres types de serveurs AAA, moins répandus : TACACS, TACACS+ ou encore Diameter. Ce dernier est défini dans la RFC 3588 ; il s'agit d'une version améliorée du protocole RADIUS[2], mais il n'est pas encore très utilisé aujourd'hui.

1. Nous avons brièvement présenté les PoP au chapitre 8.
2. Notez le subtil jeu de mot : *radius* signifie « rayon » et *diameter* bien sûr signifie « diamètre ».

Conclusion

Le protocole RADIUS offre donc trois fonctions essentielles : l'authentification des utilisateurs, le paramétrage fin et dynamique de leurs autorisations, enfin la comptabilisation précise de leurs connexions. Avant de choisir un serveur RADIUS particulier, il faut s'assurer qu'il gère bien les méthodes d'authentification que l'on souhaite mettre en œuvre et qu'il possède les connecteurs dont on peut avoir besoin, par exemple pour le relier à un contrôleur de domaine de Windows NT.

Le serveur RADIUS nous intéresse particulièrement dans le contexte du WiFi car il est le standard de fait pour le serveur d'authentification de l'architecture 802.1x. Or, nous avons vu que cette architecture était à la base des solutions de sécurité WPA Enterprise et WPA2 Enterprise (voir le chapitre 9). Nous allons donc maintenant détailler un peu plus le protocole RADIUS et montrer comment le 802.1x et le RADIUS fonctionnent ensemble.

10.2 LE PROTOCOLE RADIUS

10.2.1 Le RADIUS et l'UDP

Rappels sur UDP et TCP

L'ensemble du protocole RADIUS repose sur le protocole *User Datagram Protocol* (UDP), défini dans la RFC 768. Celui-ci fournit un service assez limité au-dessus du protocole IP[1], défini dans la RFC 791. En deux mots, le protocole UDP permet d'envoyer des paquets autonomes, qu'on appelle les *datagrams*, en utilisant un réseau IP quelconque, comme Internet, bien sûr. Le protocole UDP est très limité :

- il n'assure pas que l'ordre des paquets envoyés sera le même à l'arrivée ;
- il n'assure même pas que les paquets arriveront à destination !
- la taille des paquets est limitée à 64 kilo-octets (ko), au maximum.

À titre de comparaison, le protocole TCP, défini dans la RFC 793, repose également sur le protocole IP, mais il garantit la livraison des paquets grâce à un système d'accusés de réception ; il assure également que l'ordre des paquets sera conservé, en numérotant chaque paquet et en les réordonnant au besoin à l'arrivée. En outre, TCP permet d'envoyer des données aussi longues que voulu : il s'occupe lui-même de découper les données en multiples fragments et de reconstituer les données à l'arrivée. Il gère automatiquement le débit et contrôle la vitesse d'émission en fonction de la vitesse de transfert mesurée. Il assure enfin une connexion « virtuelle », appelée un *socket*, pour les couches réseau supérieures : ces dernières commencent par « ouvrir » un *socket* TCP avec une autre machine, puis il leur suffit d'écrire ou de lire des octets dans ce *socket*, sans avoir à se soucier de la façon dont leurs données seront regroupées en paquets, ni du moment précis auquel ces paquets seront envoyés.

1. Si vous avez besoin d'un rappel au sujet des réseaux IP, consultez l'annexe A sur le site de l'ouvrage *www.livrewifi.com*.

Bref, c'est un protocole très complet et pratique pour les couches supérieures. C'est la raison pour laquelle la plupart des protocoles d'Internet reposent sur TCP : c'est le cas notamment de HTTP (navigation Internet), SMTP (envoi d'e-mails), POP (téléchargement d'e-mails) ou encore FTP (transfert de fichiers). Cependant, toutes ces fonctionnalités ont un coût : le fait d'ouvrir un *socket* suppose une petite négociation initiale qui implique quelques allers-retours. Si tout ce que l'on veut faire est d'envoyer un simple paquet de données, de temps en temps, le protocole TCP peut être vu comme trop lourd.

À l'inverse, UDP est un protocole très simple, mais très rapide. C'est pour cette raison qu'il a été choisi comme base pour le protocole RADIUS[1]. Si un paquet RADIUS envoyé par le NAS est perdu pendant son trajet vers le serveur, le NAS réessaie tout simplement au bout de quelques secondes. Le délai entre deux tentatives, ainsi que le nombre maximal de tentatives possibles avant l'abandon, peuvent être configurés dans la plupart des NAS. Il est généralement possible de configurer chaque NAS en lui indiquant un serveur RADIUS secondaire, à contacter en cas d'échec du serveur RADIUS primaire (fig. 10.5).

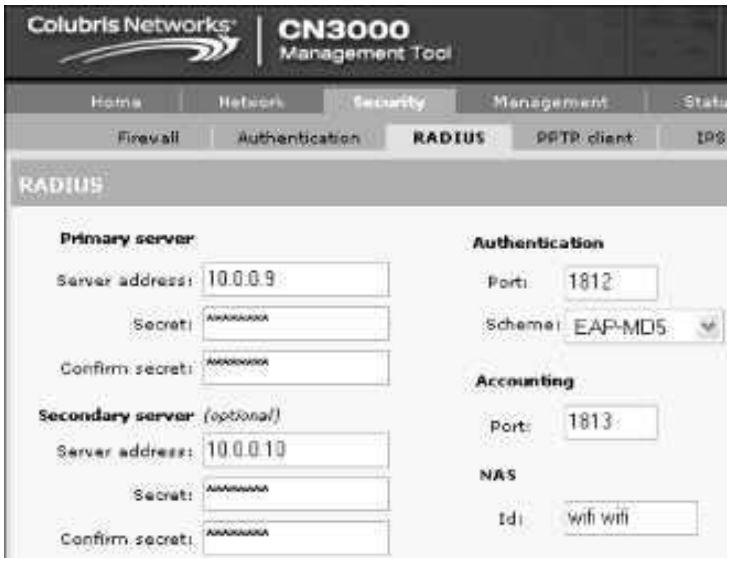


Figure 10.5 — Exemple de configuration RADIUS d'un NAS.

Les ports UDP officiels de RADIUS

L'apport principal du protocole UDP, par rapport au protocole IP, est la notion de « port ». Il s'agit d'un nombre compris entre 1 et 65 535, inclus. Chaque paquet UDP possède un port de destination et un port d'origine. Lorsqu'un paquet est reçu par une machine, seul un logiciel à l'écoute sur le port auquel est adressé le paquet le recevra.

1. Le protocole Diameter (le « nouveau RADIUS ») est revenu sur ce choix : il repose sur TCP.

Ceci permet de déployer plusieurs services UDP sur la même machine, distingués par leur port. Certains ports sont théoriquement réservés pour des services donnés[1]. C'est le cas du service RADIUS :

- le service d'authentification et d'autorisation RADIUS doit (en principe) être configuré pour écouter les paquets UDP sur le port 1812 ;
- le service de comptabilisation RADIUS doit écouter sur le port 1813.

Lorsque vous configurez un NAS pour qu'il utilise tel ou tel serveur RADIUS, vous devez donc indiquer l'adresse IP du serveur RADIUS, ainsi que le port du service d'authentification et d'autorisation et le port du service de comptabilisation.

Notez que les ports officiels ont changé depuis quelques années : ils s'agissait auparavant des ports UDP 1645 et 1646, ce qui explique pourquoi ces valeurs apparaissent encore parfois dans certains vieux équipements.

10.2.2 Les six types de paquets

Le protocole RADIUS sert aux échanges entre le NAS et le serveur RADIUS. Il spécifie six types principaux de paquets[2] (fig. 10.6) :

- Le paquet *Access-Request* est envoyé par le NAS lorsqu'un client doit être authentifié pour accéder au réseau. Ce paquet contient entre autres l'identifiant de l'utilisateur ainsi que la preuve de son identité (un mot de passe par exemple).
- Un paquet *Access-Challenge*, contenant un défi, peut être renvoyé par le serveur en réponse à un paquet *Access-Request*. Ceci est utile si la méthode d'authentification de l'utilisateur fait intervenir un défi, ou plus généralement plusieurs allers-retours entre le NAS et le serveur. Le NAS doit alors poursuivre l'authentification en renvoyant un nouveau paquet *Access-Request* au serveur, contenant la réponse au défi. Le serveur peut éventuellement renvoyer à nouveau un paquet *Access-Challenge* et ainsi de suite.
- Le paquet *Access-Accept* est renvoyé au NAS par le serveur, pour indiquer que l'utilisateur est autorisé à accéder au réseau. Ce paquet peut contenir des attributs définissant les autorisations de l'utilisateur, comme par exemple l'attribut *Session-Timeout*.
- Le paquet *Access-Reject* est bien sûr envoyé au NAS si l'utilisateur n'est pas autorisé à accéder au réseau. Ce paquet peut également transporter divers attributs, par exemple un message d'erreur à présenter à l'utilisateur.
- Le paquet *Accounting-Request* est envoyé par le NAS pour indiquer au serveur le début (type Start) ou la fin (type Stop) d'une session. Il contient toutes sortes d'attributs donnant des informations au sujet de la session : *Acct-Input-Octets*,

1. Le protocole TCP possède également la même notion de port. Par exemple, le port officiel pour le protocole HTTP est le port 80.

2. Quelques autres types de paquets RADIUS sont définis par d'autres RFC, mais ils sont moins cruciaux.

Acct-Session-Time, *User-Name*, etc. Ce paquet peut éventuellement être envoyé régulièrement au cours de la session (type *Interim-Update*).

- Enfin, le paquet *Accounting-Response* est renvoyé par le serveur pour indiquer qu'il a bien reçu le paquet *Account-Request*.

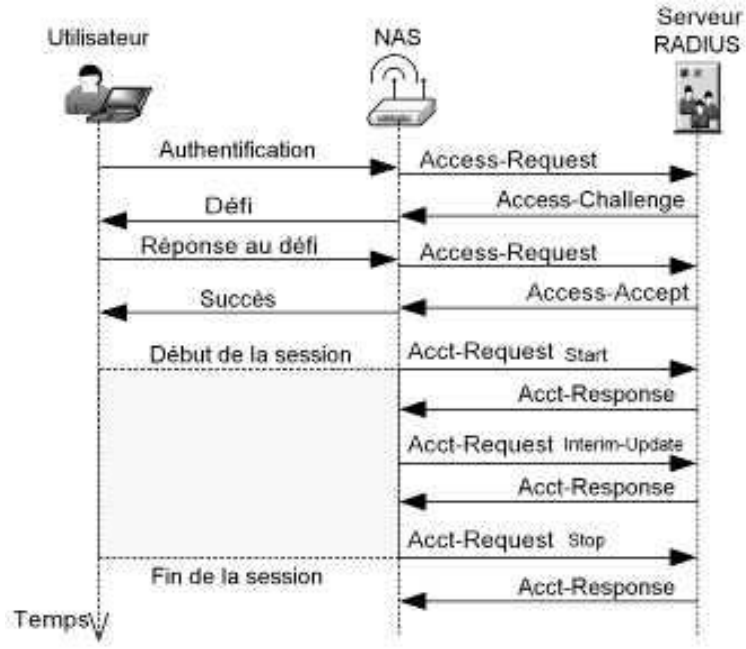


Figure 10.6 — Un scénario de communication RADIUS.

10.2.3 Le format des paquets RADIUS

L'en-tête RADIUS

Le protocole RADIUS hérite sa souplesse du format de ses paquets. En effet, chaque paquet est constitué d'un en-tête fixe et d'une liste variable d'attributs :

Code	ID	Longueur	Authenticator	Attributs
1 octet	1 octet	2 octets	16 octets	0 à 4 076 octets

- le code indique le type du paquet RADIUS : *Access-Request*, *Access-Challenge*, *Access-Accept*, *Access-Reject*, *Accounting-Request ou Accounting-Response* ;
- l'ID est inclus dans chaque requête : il s'agit d'un simple compteur qui identifie le paquet. Ceci permet notamment de savoir à quelle requête correspond une réponse RADIUS (car avec le protocole UDP, l'ordre des paquets peut changer entre l'émetteur et le récepteur) ;

- la longueur est celle du paquet au complet, en comptant l'en-tête RADIUS et les attributs ;
- l'*authenticator* (ou « sceau électronique ») sert au contrôle d'intégrité du paquet, c'est-à-dire pour s'assurer que le paquet n'a pas été modifié par un pirate entre l'émetteur et le récepteur : nous y reviendrons plus loin lorsque nous parlerons de la sécurité RADIUS ;
- enfin, les attributs sont simplement placés les uns à la suite des autres.

Les attributs

Le format de chaque attribut est très simple. Chaque attribut précise son type, sa longueur et, bien entendu, sa valeur :

Type	Longueur	Valeur
1 octet	1 octet	0 à 253 octets

- les types possibles sont définis dans la RFC 2865 et dans toutes les autres RFC liées au protocole RADIUS (2866, 2867, 2868, 2809, 2869 et 2548). Par exemple, le type *Session-Timeout* dont nous avons parlé plus haut porte le numéro 27, le type *User-Name* porte le numéro 1 et ainsi de suite ;
- la longueur est celle de l'ensemble de l'attribut, pas uniquement de la valeur ;
- la valeur peut être un nombre (sur 32 bits), une série d'octets, un texte, une adresse IP ou encore une date. Cela dépend du type de l'attribut.

Puisque le type est représenté sur un seul octet, il n'y a que 256 types possibles. C'est très peu si l'on considère que de nombreux constructeurs définissent leurs propres attributs. Pour éviter que tous les types possibles ne soient vite épuisés, la RFC 2865 définit un type spécial pour les attributs spécifiques à des constructeurs : l'attribut *Vendor-Specific* (type numéro 26). La valeur de cet attribut commence par un numéro de 32 bits qui correspond à l'identifiant du constructeur. Par exemple, le numéro attribué au constructeur Colubris est le 8744. Le reste de la valeur a un format spécifique au constructeur. En général, il s'agit d'une séquence d'attributs spécifiques au constructeur, les uns à la suite des autres :

Type (26)	Longueur	ID du constructeur	Sous-attributs spécifiques
1 octet	1 octet	4 octets	0 à 249 octets

Les « sous-attributs » ont le format habituel Type-Longueur-Valeur (TLV), mais leur type est spécifique au constructeur.

Le dictionnaire

Avec les centaines d'attributs RADIUS possibles, définis par des dizaines de constructeurs, il est parfois difficile de s'y retrouver. Surtout, il faut pouvoir configurer relativement simplement le serveur RADIUS, sans avoir à chaque fois à rechercher à quel numéro correspond le type *Session-Timeout* ou le constructeur Colubris, par exemple. Pour cela, les serveurs RADIUS ont en général un « dictionnaire », qui établit l'association entre un nom « clair », comme « Session-Timeout » et le numéro auquel il correspond dans le standard. De cette façon, lorsque vous configurez un serveur RADIUS, vous pouvez écrire des choses comme « Session-Timeout=3600 » plutôt que « Attribut 27=3600 ». C'est tout de même plus clair !

Le seul problème avec le dictionnaire est qu'il faut parfois le mettre à jour. Par exemple, si vous installez un serveur RADIUS et que deux ans plus tard vous installez un nouveau matériel, produit par un nouveau constructeur, il faudra vous assurer que le dictionnaire de votre serveur contienne bien le code de ce constructeur et les types spécifiques que vous souhaitez utiliser. Si ce n'est pas le cas, il faudra consulter le constructeur pour qu'il vous fournisse son identifiant et les définitions de ses types d'attributs.

Enfin, si vous écrivez « Session-Timeout=3600 » dans votre configuration RADIUS, comment le serveur doit-il savoir si « 3600 » doit être interprété comme un nombre ou comme du texte ? Pour résoudre ce problème, le format de chaque type d'attribut est inclus dans le dictionnaire et indique s'il s'agit d'un nombre, d'une série d'octets, d'un texte, d'une date ou d'une adresse IP.

> Le dictionnaire d'un serveur RADIUS contient la liste des attributs possibles et, pour chacun d'entre eux, son code, son format, parfois ses valeurs possibles et, s'il s'agit d'un attribut « vendor-specific », le nom et le code du constructeur qui l'a défini.

10.2.4 Le 802.1x et le RADIUS

Une architecture commune

Le protocole 802.1x décrit la même architecture que le RADIUS : un utilisateur, un contrôleur d'accès (le NAS) et un serveur d'authentification (le serveur RADIUS). Le 802.1x décrit comment l'utilisateur et le serveur doivent communiquer : avec des paquets EAP. Il précise également que le client et le contrôleur d'accès doivent être sur un même réseau local et il impose le protocole EAPoL pour transporter les paquets EAP entre l'utilisateur et le contrôleur d'accès. En revanche, il laisse le choix du protocole qui sera utilisé pour transporter les paquets EAP entre le contrôleur d'accès et le serveur d'authentification.

De son côté, le protocole RADIUS décrit la même architecture à trois acteurs. Cependant, contrairement au 802.1x, il n'impose absolument rien au sujet de la conversation entre l'utilisateur et le NAS : ils peuvent s'échanger les informations

d'authentification en utilisant le protocole PPP, avec HTTPS[1] ou encore avec EAPoL, cela n'affecte pas le RADIUS. En revanche, le protocole RADIUS définit précisément comment le NAS et le serveur RADIUS doivent communiquer : ils doivent utiliser des paquets RADIUS et se les échanger grâce au protocole UDP/IP, comme nous l'avons vu.

Les attributs EAP

Le 802.1x et le RADIUS étant conçus pour la même architecture et étant finalement assez complémentaires, ils se marient très bien. Le protocole 802.1x suggère d'ailleurs fortement l'utilisation d'un serveur RADIUS comme serveur d'authentification. Voici comment les deux protocoles fonctionnent ensemble (fig. 10.7) :

- l'utilisateur et le contrôleur d'accès dialoguent avec le protocole 802.1x, c'est-à-dire en utilisant le protocole EAPoL ;
- les paquets EAP que le contrôleur d'accès doit échanger avec le serveur sont véhiculés au sein de paquets RADIUS, contenant des « attributs EAP » prévus à cet effet ;
- en reposant sur les protocoles EAPoL et RADIUS pour le transport des paquets, l'utilisateur et le serveur dialoguent selon le protocole EAP.

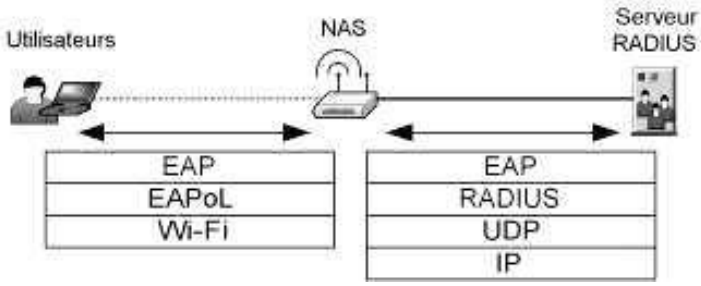


Figure 10.7 — Une architecture 802.1x avec un serveur RADIUS.

L'utilisation du protocole EAP sur RADIUS est détaillée dans la RFC 2869. C'est elle qui définit l'attribut RADIUS qui nous intéresse : l'attribut *EAP-Message* (type numéro 79). Cet attribut contient tout simplement un paquet EAP. Pour être plus précis, puisqu'un attribut RADIUS ne peut pas être plus long que 253 octets, plusieurs attributs EAP-Message peuvent se succéder pour former un paquet EAP complet.

Dans le cas de la méthode EAP/TLS et des autres méthodes de tunnel reposant sur TLS, le client et le serveur doivent s'échanger leurs certificats. Or, un certificat peut être plus grand qu'un paquet RADIUS, qui ne peut transporter que 4 076 octets

1. Au chapitre 4, nous avons vu que dans les *hotspots*, la communication entre l'utilisateur et le contrôleur d'accès reposait généralement sur une navigation web sécurisée (HTTPS). Dans ce contexte, le protocole 802.1x n'est que peu utilisé, car la configuration nécessaire découragerait de nombreux clients potentiels, alors que tout le monde possède un navigateur Web et sait l'utiliser.

(en comptant les en-têtes des attributs). Heureusement, la méthode EAP/TLS (et les autres méthodes véhiculant des données volumineuses) définit comment fragmenter le certificat et l'échanger dans plusieurs paquets EAP : le problème ne se pose donc pas.

Finalement, tout se passe de façon assez transparente. Il suffit donc de s'assurer que le serveur gère bien les méthodes EAP que l'on a choisi d'utiliser et que le contrôleur d'accès (c'est-à-dire l'AP dans le contexte du WiFi) gère bien le 802.1x et le RADIUS. Tout produit certifié WPA Enterprise devrait convenir.

Une architecture WPA Enterprise

Maintenant que nous savons comment le 802.1x et le RADIUS fonctionnent ensemble, résumons les éléments qu'il faut vérifier lorsque l'on veut déployer un réseau WiFi sécurisé avec le WPA Enterprise :

- l'utilisateur doit posséder un logiciel de connexion compatible avec le 802.1x et avec les méthodes EAP que l'on souhaite utiliser[1]. Ce logiciel doit également être compatible avec le WPA ou le WPA2 ;
- les AP doivent être compatibles avec le 802.1x, le RADIUS et le WPA ou le WPA2 : tout AP certifié WPA Enterprise conviendra ;
- le serveur RADIUS doit être capable de gérer les méthodes d'authentification EAP que l'on a choisies.

10.3 QUESTIONS DE SÉCURITÉ

10.3.1 Le secret RADIUS

Le protocole RADIUS met en œuvre quelques mécanismes assez simples (pour ne pas dire simplistes) pour protéger les informations sensibles qu'il véhicule et plus généralement pour assurer la sécurité du lien entre les contrôleurs d'accès et le serveur RADIUS.

À la base de la sécurité du protocole RADIUS, il y a le « secret » RADIUS : il s'agit d'un long mot de passe (une « passphrase ») connu à la fois du serveur RADIUS et d'un contrôleur d'accès.

> Il est très fortement recommandé de choisir un secret partagé aussi long et complexe que possible (si possible parfaitement aléatoire), différent pour chaque contrôleur d'accès.

Lors de la configuration du contrôleur d'accès (dans notre cas, le point d'accès WiFi), il faut saisir manuellement le secret RADIUS. Du côté du serveur, il faut configurer la liste des contrôleurs d'accès et saisir leurs secrets respectifs. Bien entendu,

1. Les systèmes d'exploitation récents incluent une interface 802.1x avec plusieurs méthodes EAP (EAP/TLS, PEAP/MS-CHAP-v2...).

puisque les secrets doivent être enregistrés sur le serveur, il faut s'assurer que la configuration du serveur RADIUS ne soit accessible qu'à quelques personnes de confiance.

Le secret RADIUS est utilisé à la fois pour crypter certains attributs et également pour calculer le code de contrôle d'intégrité du paquet que le récepteur utilise pour s'assurer que le paquet RADIUS n'a pas été modifié. Commençons par voir le contrôle d'intégrité, mis en œuvre par l'*authenticator*.

10.3.2 L'authenticator

Calcul de l'authenticator

L'*authenticator* (c'est-à-dire le « sceau électronique », ou si vous préférez, la signature) est un champ de 16 octets (128 bits), présent dans chaque paquet (voir § 10.2.3).

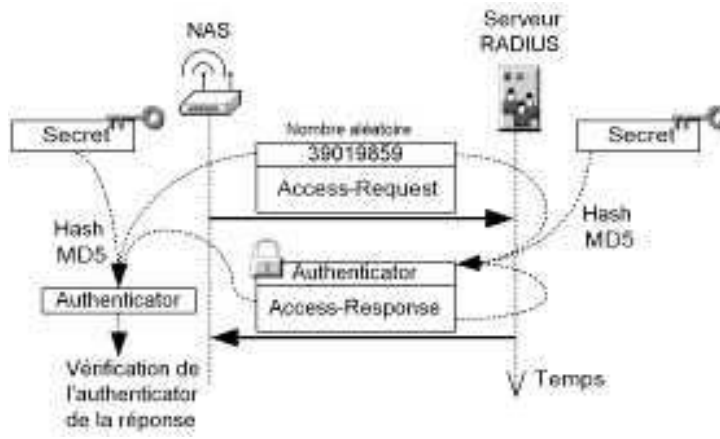


Figure 10.8 — Le rôle de l'*authenticator*.

Il fonctionne de la façon suivante (fig. 10.8) :

- lorsqu'un paquet *Access-Request* est envoyé, son *authenticator* est simplement un nombre aléatoire[1], choisi par le contrôleur d'accès ;
- dans les paquets de réponse (*Access-Challenge*, *Access-Accept* et *Access-Reject*), l'*authenticator* est calculé en utilisant l'algorithme de *hash* MD5 (voir le chapitre 8) appliqué au paquet de réponse complet, à l'*authenticator* du paquet *Access-Request*, et au secret RADIUS.

L'intérêt de ce mécanisme est le suivant : lorsque le contrôleur d'accès reçoit la réponse du serveur RADIUS, il peut vérifier la valeur de l'*authenticator* et la valider.

1. En réalité, les nombres « aléatoires » générés par un système informatique sont en général « pseudo-aléatoires », c'est-à-dire qu'ils sont issus d'un calcul complexe qui donne un résultat difficile à prévoir.

Dans ce cas, puisque le secret RADIUS est utilisé dans le calcul, il sait que c'est bien une réponse provenant du serveur. D'autre part, puisque le nombre aléatoire qu'il avait généré dans la requête est utilisé également dans le calcul, il sait qu'il s'agit bien de la réponse à cette requête et non de la réponse à une ancienne requête : cela évite les attaques de relecture. Enfin, puisque l'ensemble du paquet de réponse fait aussi partie du calcul de l'*authenticator*, il sait que le paquet de réponse n'a pas été modifié par un pirate.

Voici le détail du calcul de l'*authenticator* des paquets de réponse (où « || » signifie « suivi de ») :

$$Auth_{réponse} = MD5\ (Code \parallel ID \parallel Longueur \parallel Auth_{requête} \parallel Attributs \parallel secret)$$

Pour les paquets de comptabilisation, le processus est légèrement différent : l'*authenticator* du paquet de requête *Accounting-Request* n'est pas aléatoire. Il est calculé selon la formule précédente, avec une petite différence : puisqu'il ne s'agit pas d'une réponse à une requête, le champ $Auth_{requête}$ est remplacé par un champ nul :

$$Auth_{acct\text{-}request} = MD5\ (Code \parallel ID \parallel Longueur \parallel 16\ octets\ nuls \parallel Attributs \parallel secret)$$

De cette façon, le serveur RADIUS peut vérifier la signature des paquets *Accounting-Request* qu'il reçoit. Les paquets *Accounting-Response* sont signés de la façon habituelle, en calculant un *hash* MD5 à partir du paquet au complet, du secret et de l'*authenticator* de la requête.

Cryptage des mots de passe

L'*authenticator* et le secret RADIUS sont également utilisés pour crypter les simples mots de passe, pour les méthodes d'authentification les plus simples (PAP, CHAP...), mais pas pour les méthodes EAP. A titre d'exemple, voici comment se déroule le cryptage pour un mot de passe PAP :

- le mot de passe P est découpé en blocs de 16 octets : P_1, P_2, P_3...
- si le dernier bloc est plus court que 16 octets, il est complété avec des zéros ;
- le premier bloc C_1 du mot de passe crypté C est calculé de la façon suivante : $C_1 = MD5\ (Secret \parallel Auth_{requête}) \approx P_1$ ($\approx$ est l'opération XOR)
- $C_2 = MD5\ (Secret \parallel C_1) \oplus P_2$
- $C_3 = MD5\ (Secret \parallel C_2) \oplus P_3$
- ...

Ce cryptage ressemble un peu à l'algorithme RC4 (voir le chapitre 7, § 7.2) : un flux pseudo-aléatoire est généré grâce à l'algorithme de *hash* MD5 et ce flux est combiné avec les données à crypter (en l'occurrence le mot de passe) par le biais de l'opération XOR. Ce cryptage fonctionne bien, mais il est critiqué car il utilise l'algorithme MD5 comme source de flux pseudo-aléatoire, or il n'a pas été conçu pour cela, mais pour générer des *hash*, c'est-à-dire des codes de contrôle d'intégrité.

Notons que la plupart des attributs sont envoyés « en clair ». Seuls les mots de passe simples et un ou deux attributs sensibles sont cryptés, en général d'une façon

similaire à ce que nous venons de présenter. Notons que les attributs EAP-Message ne sont pas cryptés par le protocole RADIUS. Heureusement, les méthodes EAP elles-mêmes protègent le contenu des paquets.

> La plupart des attributs RADIUS sont envoyés « en clair ». Seuls les attributs les plus sensibles sont cryptés en utilisant le secret RADIUS.

Les défauts de l'authenticator

L'*authenticator* du protocole RADIUS protège les mots de passe simples et il lutte efficacement contre la majorité des attaques de relecture ou de modification des paquets. Malheureusement, il possède des faiblesses importantes :

- D'une part, le paquet *Access-Request* contient un *authenticator* aléatoire, donc il n'est pas signé. Ceci permet à un pirate d'envoyer au serveur RADIUS autant de paquets de ce type qu'il le souhaite, en se faisant passer pour un NAS.
- D'autre part, l'*authenticator* du paquet *Accounting-Request* ne contient pas de partie aléatoire, donc si le contrôleur d'accès envoie deux paquets de ce type de contenus identiques, leurs champs *authenticator* seront eux-mêmes identiques. Un pirate peut donc enregistrer des paquets *Accounting-Request* et les « rejouer » plus tard. Toutefois, puisque les paquets contiennent un identifiant unique pour chaque session (*Acct-Session-Id*) et qu'une session commence par un seul paquet de départ (type Start) et se termine par un seul paquet de fin (type Stop), les paquets de type Start ou Stop répétés par un pirate seront rejetés par le serveur. En revanche, les paquets de type Interim-Update peuvent être répétés, ce qui peut endommager les historiques de connexion. Seule protection : le champ ID, car il change à chaque paquet. Le serveur vérifie généralement que l'ID du paquet qu'il reçoit est proche de l'ID du dernier paquet qu'il a reçu. Il pourra ainsi rejeter tous les paquets de relecture dont l'ID est incohérent. Toutefois, cet ID n'a qu'une longueur de 8 bits, donc seulement 256 valeurs possibles. Ainsi, le pirate peut rejouer les paquets *Interim-Update* environ tous les 256 paquets envoyés par le contrôleur d'accès ;
- Les attaques de relecture contre les paquets de type Interim-Update peuvent également être dirigées contre le contrôleur d'accès : le pirate peut capturer un paquet *Accounting-Response* de type *Interim-Update* renvoyé par le serveur RADIUS et le rejouer ultérieurement. Ceci peut lui permettre de faire croire au contrôleur d'accès que le serveur a bien reçu son paquet Accounting-Request, même si ce n'est pas le cas.

Les attaques contre les paquets Interim-Update sont possibles, mais elles entraînent davantage un désagrément qu'une importante faille de sécurité. Le problème le plus grave est le premier, car il signifie qu'un pirate peut, à loisir, modifier un paquet émis par un contrôleur d'accès ou émettre lui-même des paquets de type Access-Request. Ceci peut lui permettre de chercher le mot de passe d'un utilisateur, en essayant des

milliers de possibilités[1]. Pour pallier ce problème, un nouvel attribut a été défini : le *Message-Authenticator*. Il ne résout cependant pas le problème de la répétition des paquets de comptabilisation Interim-Update.

10.3.3 L'attribut Message-Authenticator

Cet attribut est défini dans la RFC 2869, qui décrit comment utiliser EAP dans des paquets RADIUS. Lorsqu'un paquet RADIUS contient un attribut EAP-Message, il doit obligatoirement contenir un attribut *Message-Authenticator*. Sinon, cet attribut est optionnel.

Le *Message-Authenticator* contient un code de contrôle d'intégrité calculé par un *hash* de type HMAC-MD5[2] sur l'ensemble du paquet à envoyer, plus le secret RADIUS et l'*authenticator* de la requête (attention, il s'agit du *champ authenticator* de la requête, pas de son *attribut Message-Authenticator*) :

$$\text{Msg-Auth} = \text{HMAC-MD5 (Code} \,||\, \text{ID} \,||\, \text{Longueur} \,||\, \text{Auth}_{\text{requête}} \,||\, \text{Attributs, secret)}$$

Le calcul est le même pour tout type de paquet, qu'il s'agisse d'une requête ou d'une réponse : le champ *authenticator* utilisé dans le calcul est toujours celui de la requête, qui est aléatoire dans le cas d'un Access-Request.

Grâce au *Message-Authenticator*, les paquets Access-Request sont signés correctement et le serveur peut donc rejeter les paquets modifiés ou créés par des pirates.

Toutefois, rien n'empêche un pirate de capturer un paquet Access-Request et d'enlever l'attribut *Message-Authenticator*. La RFC 2869 stipule toutefois que le serveur doit obligatoirement rejeter les paquets contenant un attribut EAP-Message mais pas d'attribut *Message-Authenticator*, donc en principe, si une méthode EAP est utilisée, cette attaque n'est pas possible. En revanche, si l'on n'utilise pas une méthode d'authentification EAP, le serveur risque d'accepter les paquets sans *Message-Authenticator*. Heureusement, dans le contexte du WiFi avec une architecture WPA Enterprise, on utilise bien une méthode EAP, donc on est protégé.

> Lorsque l'on utilise une authentification EAP, ce qui est le cas avec l'architecture WPA Enterprise, l'attribut *Message-Authenticator* protège les paquets Access-Request contre les modifications d'un pirate.

10.3.4 L'attaque hors-ligne contre le secret

L'un des problèmes avec la sécurité du protocole RADIUS telle qu'elle est mise en œuvre est que le secret est vulnérable à une attaque de type dictionnaire hors-ligne.

1. C'est une attaque de dictionnaire en ligne, donc le serveur peut mettre en œuvre un mécanisme pour bloquer les multiples tentatives infructueuses.
2. L'algorithme HMAC est défini dans la RFC 2104. Il décrit comment calculer un hash avec MD5 (ou toute autre fonction de hash) sur un message dont on veut contrôler l'intégrité et une clé (le secret).

En effet, si le pirate peut capturer un paquet RADIUS quelconque, il peut essayer, chez lui (c'est-à-dire sans avoir à se connecter au réseau), de trouver le secret RADIUS : il lui suffit pour cela d'essayer des milliers de secrets possibles, jusqu'à trouver le secret qui produit le bon champ *authenticator* (sauf pour les paquets *Access-Request*) ou le bon attribut *Message-Authenticator*.

Puisqu'une attaque de dictionnaire hors-ligne est réalisable, la recommandation habituelle est de mise : choisir des secrets aussi longs et complexes que possible. Si le pirate parvient à récupérer le secret, il pourra se faire passer pour un contrôleur d'accès auprès du serveur RADIUS, ou pour le serveur RADIUS auprès du contrôleur d'accès. Si le même secret est utilisé pour tous les contrôleurs d'accès, il pourra attaquer tous les contrôleurs d'accès : c'est pourquoi l'on recommande d'utiliser un secret différent pour chaque contrôleur d'accès (c'est-à-dire pour chaque AP).

10.3.5 Le RADIUS sur Internet

Les NAS sont identifiés par leur adresse IP

Puisque tous les contrôleurs d'accès utilisent potentiellement des secrets différents, le serveur RADIUS doit déterminer de quel contrôleur d'accès provient un paquet pour pouvoir savoir quel secret utiliser. Pour cela, on pourrait imaginer d'utiliser l'attribut NAS-Identifier dont nous avons parlé plus haut, mais le protocole RADIUS impose une autre méthode : le NAS doit être identifié par son adresse IP. Pour cela, l'adresse IP source de chaque paquet RADIUS doit être utilisée par le serveur.

L'avantage de cette solution est qu'un serveur RADIUS pourra très facilement filtrer les paquets qu'il reçoit en rejetant tous ceux dont l'adresse IP source ne correspond pas à un NAS connu.

> Dans la configuration du serveur RADIUS, les NAS sont identifiés par leur adresse IP.

Le NAT : quelques rappels

Malheureusement, l'identification des NAS pas leur adresse IP provoque quelques problèmes ennuyeux. Voyons lesquels.

Si un NAS est installé dans un réseau d'entreprise, il aura sans doute une adresse IP locale, du type 10.0.20.3 ou encore 192.168.0.5. Si le serveur RADIUS ne se trouve pas sur le même réseau local et que les paquets RADIUS doivent passer directement par Internet, alors au moment de « sortir » vers Internet, la passerelle (par exemple, le modem-routeur, dans le cas d'une connexion ADSL) modifiera l'adresse IP source du paquet pour lui donner sa propre adresse IP « publique » sur Internet (par exemple 213.91.4.193) : ceci permettra au serveur d'envoyer sa réponse au bon endroit. On appelle cela du *Network Address Translation* (NAT), c'est-à-dire de la translation d'adresse. Plus précisément, il s'agit dans ce cas de Source-NAT (SNAT), puisque c'est l'adresse IP source qui est modifiée.

Lorsque le serveur RADIUS reçoit le paquet, il ne voit pas l'adresse locale du NAS, mais son adresse « publique », c'est-à-dire l'adresse de la passerelle (celle du

modem-routeur, par exemple). Le serveur doit donc être configuré pour associer le NAS à cette adresse IP publique et non à l'adresse locale du NAS. Lorsque le serveur répond à la requête, le paquet est adressé à l'adresse publique du NAS, c'est-à-dire à la passerelle. Quand la passerelle reçoit le paquet, elle se « souvient » qu'une requête provenant de telle IP locale (et tel port UDP) attendait une réponse. Elle sait donc qu'il faut rediriger cette réponse vers l'adresse IP locale (et le port) en question : elle remplace l'adresse IP de destination du paquet par l'adresse IP du NAS. On appelle cela le *Destination-NAT* (DNAT). La réponse RADIUS peut ainsi atteindre le NAS. Tout ce mécanisme de SNAT et de DNAT s'appelle le « NAT dynamique »[1] : il permet à plusieurs stations sur un même réseau local de pouvoir communiquer avec Internet au travers d'une seule adresse IP publique.

Problèmes du NAT avec le RADIUS

Le premier problème est le suivant : si plusieurs NAS sont déployés sur le même réseau local, ils auront la même adresse IP source du point de vue du serveur RADIUS, si celui-ci se trouve sur un autre réseau, au travers de l'Internet (fig. 10.9). Ils devront donc partager la même configuration sur le serveur, en particulier le même secret.

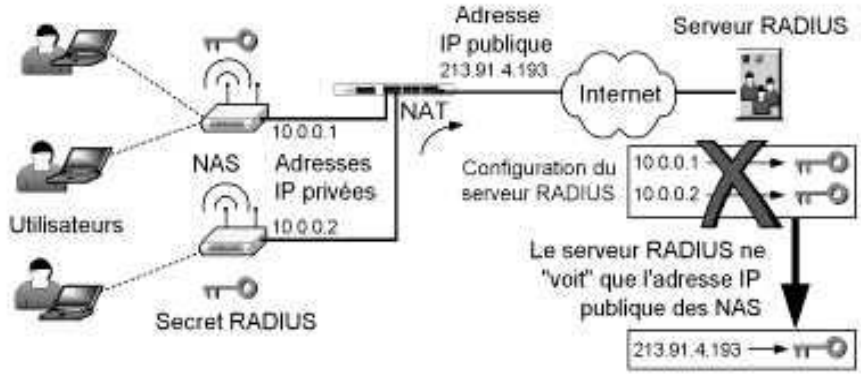


Figure 10.9 — Le problème du NAT et du RADIUS.

Le deuxième problème peut arriver si l'adresse IP publique est susceptible de changer. C'est parfois le cas si la connexion à Internet repose sur une connexion ADSL, par exemple. En effet, les fournisseurs d'accès à Internet (FAI) ne possèdent qu'un nombre limité d'adresses IP « publiques » et ils les attribuent souvent dynamiquement à leurs clients, au gré de leurs connexions. Il n'est pas rare que l'adresse IP publique d'une connexion ADSL change quotidiennement. Bien sûr, si l'adresse IP publique d'un NAS change, le serveur RADIUS ne pourra plus le reconnaître. Une solution serait de mettre en place un mécanisme qui vérifie régulièrement l'adresse IP publique

1. Par opposition au « NAT statique », où la passerelle est configurée pour que tous les paquets qui lui sont adressés sur tel port UDP ou TCP soient redirigés localement vers telle adresse IP. Ceci permet de rendre accessible sur Internet un serveur installé sur un réseau local (par exemple un serveur RADIUS ou Web).

de chaque réseau local où des NAS sont déployés et qui mette à jour automatiquement la configuration du serveur RADIUS... mais évidemment ce n'est pas la panacée !

La première solution au problème des IP dynamiques consiste simplement à demander une « IP statique » à son FAI : une adresse IP publique vous est alors attribuée et elle ne change jamais. Cela ne résout cependant pas le premier problème, car tous les NAS sur un même réseau auront encore la même adresse IP publique du point de vue du serveur.

Le risque de DoS

Il reste encore un problème important : les paquets UDP sont très utilisés pour réaliser des attaques de type déni de service (DoS) contre un réseau. Pour cela, un pirate situé n'importe où sur Internet submerge le réseau de paquets UDP inutiles. Au mieux, la connexion à Internet est lente ou indisponible, au pire, les serveurs s'arrêtent. Le protocole UDP est apprécié par les pirates car il est difficile pour un pare-feu de savoir si un paquet UDP est légitime ou non, car il n'y a pas de notion de « contexte » avec UDP, contrairement à TCP pour lequel il y a les *sockets*.

Il est recommandé de bloquer tout le trafic UDP rentrant, dans le pare-feu d'une connexion Internet (sauf s'il s'agit de réponses à des requêtes sortantes). Un serveur RADIUS ne doit donc pas être accessible directement depuis Internet.

Pour finir, il est tout à fait déconseillé d'envoyer des paquets RADIUS directement sur Internet, sans protection, car ils contiennent des informations, dont la plupart ne sont pas cryptées.

Résumons : le NAT pose problème, le pare-feu de chaque connexion à Internet doit bloquer le trafic UDP (donc le trafic RADIUS) et enfin les paquets RADIUS ne doivent pas transiter en clair sur Internet. Mais alors, comment des NAS situés sur un réseau donné peuvent-ils communiquer avec un serveur RADIUS situé sur un autre réseau (ce qui arrivera, par exemple, si votre société possède plusieurs bureaux) ? La réponse vient des Réseaux Privés Virtuels (RPV), appelés également les *Virtual Private Networks* (VPN).

Une solution : les VPN

Lorsque l'architecture RADIUS doit être distribuée sur plusieurs sites distincts, il est très recommandé de mettre en place une architecture VPN. Ces architectures sont assez complexes et ce livre n'a pas pour vocation de les décrire en détail. Nous les avons déjà mentionnées au chapitre 6, dans le § 6.3.9.

Leur principe est le suivant : ils permettent de mettre en place un réseau sécurisé en passant par des liaisons non sécurisées. Au chapitre 6, ils représentaient une option possible pour sécuriser une connexion sans fil (sans forcément utiliser le WPA ou le WPA2). Maintenant, ils peuvent également servir à relier plusieurs sites entre eux, par le biais d'Internet.

Plusieurs architectures sont possibles (fig. 10.10) : la solution la plus fréquente consiste à créer des tunnels sécurisés entre les passerelles de chaque site. Une autre

option consiste à relier directement les équipements dont les communications doivent être sécurisées à un serveur VPN. Toutes leurs communications passent alors par ce serveur et sont cryptées. Certains AP possèdent ainsi une fonction de « client VPN » (pour les protocoles PPTP, L2TP ou IPSec, généralement) : ils peuvent ainsi se connecter à un serveur VPN et tout leur trafic RADIUS est envoyé au serveur au sein d'un tunnel sécurisé. À l'arrivée, les paquets sont relayés par le serveur VPN vers le serveur RADIUS, qui peut être hébergé par la même machine. Cette solution est la plus sûre, car les paquets RADIUS sont protégés de bout en bout et ne transitent jamais « en clair ».

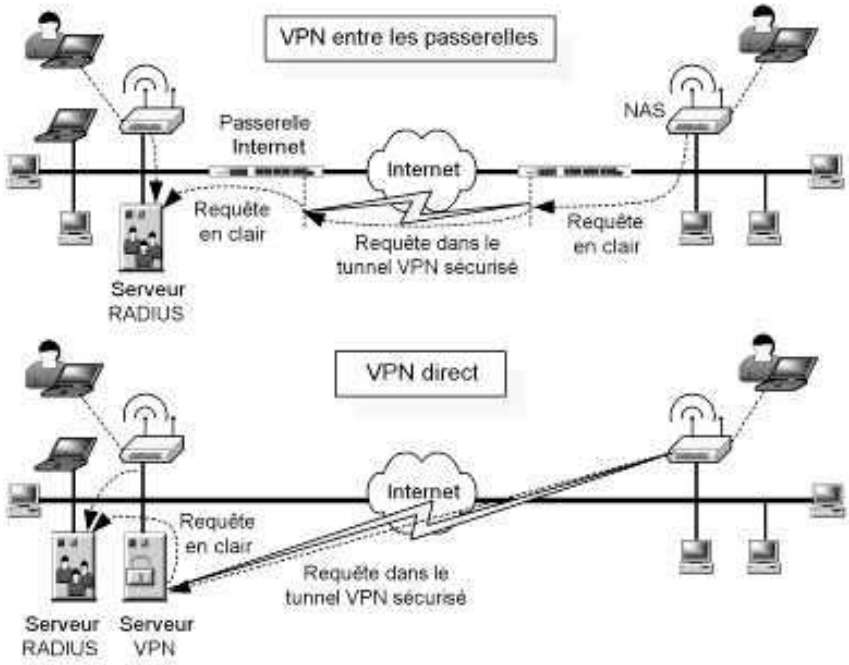


Figure 10.10 — Les architectures VPN pour un déploiement RADIUS.

Quelle que soit l'architecture VPN choisie pour relier les sites entre eux, toutes les machines auront « l'impression » d'être sur le même réseau local. Ceci permet de résoudre tous les problèmes d'adressage que nous avons mentionnés : chaque NAS apparaît bien au serveur RADIUS avec sa propre adresse IP locale. En outre, cette adresse IP ne change pas, même si l'adresse IP publique de la connexion à Internet est dynamique.

Les VPN sont généralement résistants à de nombreuses attaques de type DoS, toutes les communications sont cryptées dans les tunnels, un contrôle d'intégrité puissant est réalisé et les attaques de relecture sont impossibles. Bref, le trafic RADIUS qui transite au sein des tunnels VPN est hautement sécurisé. Sauf bien sûr si le réseau VPN est mal mis en œuvre (ce n'est pas une tâche facile).

Si le trafic RADIUS doit passer par Internet, il est fortement recommandé de mettre en place un tunnel VPN pour le sécuriser. Ce n'est malheureusement pas évident à réaliser.

10.3.6 Les VLAN

Si les AP n'intègrent pas un client VPN et que l'on choisit l'architecture VPN dans laquelle seules les passerelles sont reliées entre elles par des tunnels sécurisés, alors le trafic entre les NAS et les passerelles ne sera pas protégé par les tunnels. Plus généralement, si les NAS et le serveur RADIUS sont sur un même réseau local mais pas sur la même machine, alors le trafic RADIUS transitera en clair sur ce réseau. Si un pirate parvient à accéder au réseau local, il pourra assez facilement intercepter le trafic RADIUS, par exemple par le biais d'une attaque ARP (voir l'annexe B sur le site *www.livrewifi.com*).

Pour éviter cela, une solution consiste à placer les AP et le serveur RADIUS sur un même réseau virtuel (VLAN), isolé du reste du réseau (fig. 10.11). Malheureusement, puisque les utilisateurs doivent pouvoir se connecter aux AP, s'authentifier et accéder ensuite au réseau, les AP doivent être capables de gérer plusieurs VLAN : l'un pour les utilisateurs, l'autre pour leur connexion avec le serveur RADIUS. De nombreux AP possèdent maintenant cette option.

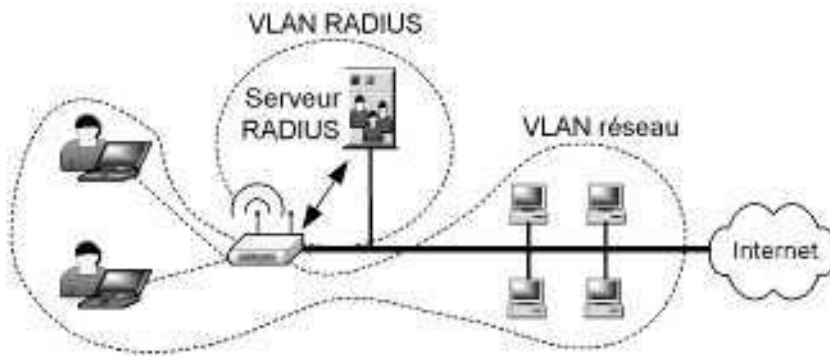


Figure 10.11 — Le trafic RADIUS isolé dans un VLAN.

10.3.7 L'échange de la clé PMK

Lorsque nous avons présenté l'architecture WPA Enterprise, nous avons précisé que le lien entre le contrôleur d'accès et le serveur d'authentification devait absolument être sécurisé. En effet, rappelez-vous, la clé maîtresse PMK, celle qui est négociée entre l'utilisateur et le serveur d'authentification, celle à partir de laquelle toutes les clés de cryptage et d'intégrité sont générées, celle sur laquelle repose la sécurité du WPA et du WPA2, bref, cette clé maîtresse doit être envoyée par le serveur RADIUS à l'AP (le contrôleur d'accès) auquel est associé l'utilisateur (fig. 10.12). Comment cette clé est-elle protégée ?

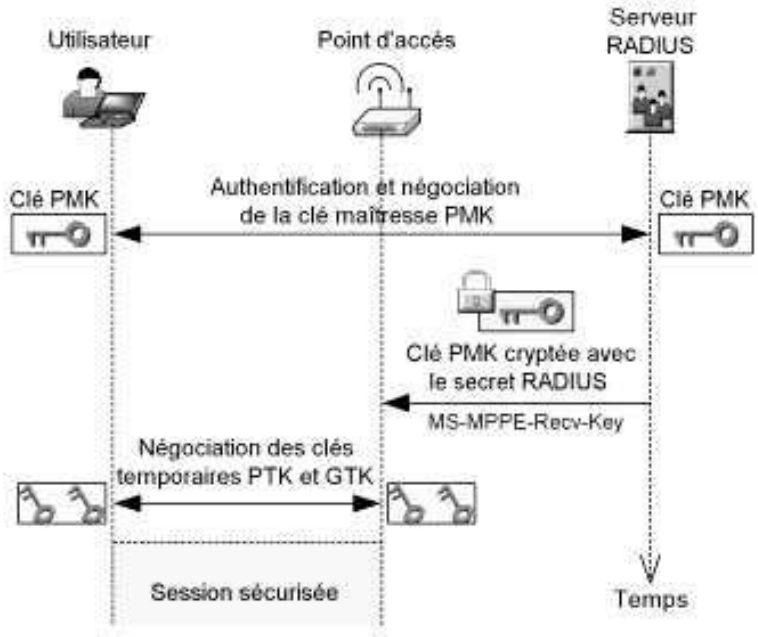


Figure 10.12 — L'envoi de la clé maîtresse PMK, du serveur RADIUS vers l'AP.

Le WPA stipule que la clé PMK doit être envoyée du serveur au NAS par le biais d'un paquet RADIUS contenant un attribut *Vendor-Specific* défini par la société Microsoft (son identifiant est le 311). L'attribut spécifique en question porte le numéro 17 et son nom (un peu obscur) est MS-MPPE-Recv-Key. Voyons pourquoi cet attribut a été choisi.

Le protocole *Microsoft Point-to-Point Encryption* (MPPE) a pour but de sécuriser une liaison PPP. Il est défini dans la RFC 3078. Par ailleurs, Microsoft a défini la RFC 2548 pour permettre l'utilisation de certaines fonctions spécifiques à Microsoft, dont quelques unes liées au protocole MPPE, avec le protocole RADIUS. Cette RFC décrit notamment comment une clé secrète peut être cryptée et intégrée dans un attribut RADIUS pour être transmise du serveur RADIUS vers un NAS : c'est là que l'attribut MS-MPPE-Recv-Key est défini.

Lorsque le groupe de travail 802.11i s'est penché sur le problème de la distribution de la clé PMK, il n'existait aucun attribut RADIUS standard réellement adapté. Ils se sont donc penchés sur les attributs spécifiques existants et l'attribut MS-MPPE-Recv-Key est apparu comme la meilleure solution. Bien que cet attribut ait été défini par Microsoft et porte ses initiales, il est décrit dans une RFC et n'est donc absolument pas « fermé ». On peut donc l'utiliser sans être lié le moins du monde à Microsoft. Notons que le WPA impose l'usage de cet attribut, alors que le WPA2 ne fournit que des recommandations, en citant notamment cet attribut.

Bref, la clé PMK est cryptée grâce à un algorithme défini dans la RFC 2548 et elle est intégrée dans un attribut RADIUS MS-MPPE-Recv-Key pour être envoyée

à l'AP (le contrôleur d'accès). L'algorithme de cryptage de la clé est très semblable à l'algorithme que nous avons présenté plus haut, pour le cryptage du mot de passe PAP. Certains estiment que ce n'est pas un cryptage exceptionnel, mais il semble suffisant. La confidentialité de l'échange est assurée par le secret RADIUS, sur lequel repose le cryptage. Il est donc évident que si le secret est compromis, toute la sécurité WPA ou WPA2 s'effondre. Au risque de nous répéter, il faut donc faire attention à utiliser des secrets RADIUS aussi longs et complexes que possible !

Résumé

Ce dernier chapitre nous a permis d'aborder en détail le protocole RADIUS et toutes les questions de sécurité qui se posent lorsqu'un serveur de ce type doit être mis en place.

L'architecture RADIUS repose sur trois types d'acteurs : les utilisateurs, les NAS et le serveur RADIUS.

Les *utilisateurs* cherchent à se connecter à un réseau (ou à tout autre service).

Les *contrôleurs d'accès*, appelés les NAS (ou encore les « clients » dans le jargon du protocole RADIUS, ce qui peut prêter à confusion), ont pour rôle de demander aux utilisateurs de s'identifier et de ne les laisser passer que s'ils sont authentifiés par le serveur RADIUS et uniquement selon leurs droits d'accès. Dans le contexte du WiFi, les NAS sont les points d'accès (AP).

Le *serveur RADIUS* a pour fonction d'authentifier les utilisateurs en répondant aux requêtes d'authentification envoyées par les NAS. Lorsqu'il informe un NAS qu'un utilisateur est bien authentifié et peut accéder au réseau, le serveur RADIUS fournit souvent des instructions variées à ce NAS, sous la forme « d'attributs ». Ces instructions peuvent indiquer qu'il faut déconnecter l'utilisateur au bout d'un certain temps, ou encore que cet utilisateur ne doit pas pouvoir accéder à telle ou telle partie du réseau. Enfin, le serveur RADIUS a également pour fonction d'enregistrer l'historique des sessions des utilisateurs. Les trois fonctions d'un serveur RADIUS se résument donc par les lettres AAA : *Authentification*, *Autorisation* et *Accounting* (comptabilisation).

Les méthodes d'authentification possibles sont très variées : PAP, CHAP, MS-CHAP, MS-CHAP-v2 ou encore toutes les méthodes EAP. Un serveur RADIUS peut être relié à divers systèmes externes d'authentification, tels que des serveurs LDAP, des contrôleurs de domaine de Windows NT ou encore d'autres serveurs RADIUS.

Le protocole RADIUS lui-même est assez simple et surtout très souple, car chaque paquet peut contenir une liste d'attributs variés. De nouveaux attributs peuvent être définis et véhiculés, sans difficulté : il suffit de les rajouter dans le « dictionnaire » du serveur RADIUS, qui contient la liste des attributs possibles, leur nom, leur numéro et leur format.

La sécurité offerte par le protocole RADIUS n'est pas exceptionnelle : un long mot de passe (le « secret ») doit être installé dans chaque NAS et être connu du serveur uniquement. Toute la sécurité du protocole RADIUS repose sur ce secret.

En outre, lorsque le serveur RADIUS reçoit un paquet, il doit déterminer quel secret a été utilisé pour le signer. Pour cela, il utilise l'adresse IP source du paquet et détermine quel NAS l'a émis. Ceci peut poser des problèmes si le trafic RADIUS passe directement par Internet (ce qui est peu recommandé) : plusieurs NAS peuvent alors être pris pour un seul ; par ailleurs les changements d'adresse IP réguliers imposés par certains FAI peuvent être gênants. Voici donc les principales recommandations de sécurité RADIUS :

– Il faut utiliser à tout prix un secret aussi long et complexe que possible (20 caractères aléatoires, par exemple), différent pour chaque NAS.

– Il faut utiliser si possible une méthode d'authentification EAP à tunnel (EAP/TLS, EAP/PEAP, EAP/TTLS ou encore EAP/FAST).

– Si les paquets RADIUS doivent passer par Internet, il faut les protéger, notamment en déployant une architecture VPN entre les sites distants.

– Si possible, le trafic RADIUS doit être isolé dans un VLAN protégé.

11

Les obligations légales

Objectif

Ce chapitre a pour but de présenter les principales obligations légales que vous devrez respecter si vous déployez une installation WiFi. Ces obligations sont de natures très différentes, avec des objectifs bien distincts et parfois contradictoires :

– protéger la vie privée des utilisateurs du réseau ;
– lutter contre la cybercriminalité ;
– permettre la cohabitation de services sans fil voisins ;
– garantir la sécurité sanitaire des personnes passant dans le périmètre de rayonnement des antennes.

Les deux premiers points sont importants mais ils ne sont pas spécifiques au WiFi, donc nous nous contenterons d'un bref rappel. En revanche, nous approfondirons davantage les deux derniers points, et surtout la question de la santé, car elle fait actuellement débat et suscite de vives inquiétudes.

11.1 PROTÉGER LA VIE PRIVÉE DES UTILISATEURS DU RÉSEAU

À la fin des années 1970, alors que l'informatique était encore réservée aux experts, la France a été le premier pays au monde à se doter de lois visant à protéger les individus contre l'utilisation abusive de leurs informations personnelles dans les systèmes informatiques. Trente ans après, ces lois sont bien rodées, avec une jurisprudence très fournie : vous avez donc fort intérêt à les respecter, car les amendes peuvent être

sévères, et en cas de manquement grave votre responsabilité pénale peut même être engagée.

Si vous stockez des informations personnelles nominatives dans votre système informatique, vous devez au préalable faire une déclaration auprès de la Commission nationale de l'informatique et des libertés (CNIL, www.cnil.fr). Vous devez ensuite mettre en œuvre les moyens nécessaires pour protéger ces informations, informer les utilisateurs du fait que vous allez enregistrer leurs informations personnelles, leur permettre de consulter ces informations et les corriger le cas échéant (en cas de changement d'adresse, par exemple), et ne pas transmettre ces informations à des tiers sans le consentement des utilisateurs.

Vous avez également l'obligation de supprimer les informations nominatives de votre système lorsqu'une personne n'utilise plus votre service : vous pouvez supprimer les données ou simplement les rendre anonymes (vous pouvez ainsi conserver des informations non nominatives, à des fins statistiques, comptables ou fiscales par exemple).

La CNIL exige que le contenu des communications soit tenu parfaitement secret. Par exemple, un employeur n'a pas le droit de lire les emails d'un employé si le titre de l'email indique qu'il s'agit d'une communication privée (mais il peut bien sûr interdire l'utilisation du système de messagerie à des fins privées).

> Pour plus de détails, nous vous invitons vivement à consulter le site web de la CNIL,www.cnil.fr.

11.2 LUTTER CONTRE LA CYBERCRIMINALITÉ

La criminalité sur Internet est malheureusement en forte croissance, et les moyens à disposition des forces de l'ordre pour lutter contre elle étaient jusqu'à récemment très insuffisants. Se sont ainsi multipliés divers « cyberdélits » que l'on peut classer en trois niveaux de gravité :

- Crime organisé, terrorisme, chantage, pédophilie...
- Arnaques « simples », fraudes à la carte bancaire, *phishing*[1]...
- Téléchargements illégaux, piratage de logiciels...

Les délits les plus graves ne représentent qu'un faible pourcentage des actes criminels sur Internet, mais ce sont eux qui causent le plus de dégâts : ce sont donc ces délits graves que visent, en premier lieu, les récentes lois contre la cybercriminalité (inversement, les délits les moins graves représentent l'immense majorité des délits sur Internet, mais ils ne sont presque pas poursuivis).

1. Le *phishing* consiste à mettre en œuvre un site web qui ressemble à un site web connu afin de piéger des utilisateurs imprudents et leur voler des informations sensibles (numéro de carte bancaire, identifiants...).

La loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme donne davantage de moyens aux forces de police pour lutter contre la cybercriminalité. Cette loi impose notamment aux Fournisseurs d'accès à Internet (FAI) de contrôler l'identité des personnes qui se connectent à leur réseau, et de conserver l'historique des connexions pendant un an. Dans le cas des opérateurs de *hotspots* WiFi, le premier point est problématique : en effet, lorsqu'un utilisateur se connecte à un *hotspot*, il ne rencontre généralement personne, et il n'est donc pas envisageable de lui demander sa carte d'identité. Les opérateurs de *hotspots* font donc souvent l'impasse complète sur cette obligation, en ne contrôlant absolument pas l'identité des utilisateurs. Certains opérateurs de *hotspots* font de leur mieux, en demandant par exemple l'adresse email de l'utilisateur (ou son numéro de téléphone mobile), puis en lui envoyant ses identifiants par email (ou par SMS). C'est mieux que rien, et pour l'instant il semble que cela soit considéré comme suffisant... mais la jurisprudence peut évoluer.

En ce qui concerne l'historique des connexions, il s'agit d'enregistrer au strict minimum l'heure de début et de fin de connexion, ainsi que l'adresse IP et l'adresse MAC de chaque utilisateur. Toute information personnelle exigée pour la fourniture du service doit être également conservée pendant un an (par exemple l'adresse email ou le numéro de téléphone mobile, s'ils sont demandés). Si vous souhaitez offrir un service de *hotspot* gratuit, cela ne vous exempte pas des obligations précédentes : même si vous choisissez de n'exiger aucune information personnelle de la part des utilisateurs, vous devrez tout de même conserver leurs historiques de connexion pendant un an.

Contrairement à ce que l'on entend parfois, il n'est pas demandé d'enregistrer le *contenu* des communications. C'est d'ailleurs interdit par la CNIL (voir § 11.1). En revanche, si vous mettez en œuvre un service de communication, par exemple un système d'emails ou de téléphonie sur IP, alors vous devez conserver pendant un an l'historique des communications : non pas le contenu des communications, mais l'heure exacte de la communication, et sa durée le cas échéant, ainsi que les coordonnées de l'émetteur et des destinataires.

Si les services de lutte contre le terrorisme en font la demande, les opérateurs doivent fournir toutes les données qu'ils possèdent sur l'utilisateur suspect : informations personnelles, adresses MAC et localisation des équipements utilisés, liste des numéros appelés et appelants, durée et date des communications, etc. La Commission nationale de contrôle des interceptions de sécurité (CNCIS) a pour rôle de contrôler ce pouvoir de police afin d'éviter les abus.

De nouvelles lois visant à lutter contre le terrorisme, le piratage, et plus généralement la criminalité sur Internet, sont régulièrement proposées : HADOPI, LOPSI puis LOPSI2, etc. Nous vous invitons donc à consulter le site web du ministère de l'Intérieur[1], ainsi que le site web LegiFrance[2] pour avoir les informations les plus récentes.

1. http://www.interieur.gouv.fr/
2. http://www.legifrance.gouv.fr/

11.3 PERMETTRE LA COHABITATION DE SERVICES SANS FIL VOISINS

11.3.1 Des bandes de fréquences libres

Les deux bandes de fréquence utilisées en WiFi, à 2,4 GHz et à 5 GHz, sont libres : chacun peut installer un point d'accès WiFi chez lui, sans avoir à payer une redevance à l'Autorité de régulation des communications électroniques et des postes (ARCEP), et sans même avoir à demander une autorisation[1]. Mais il y a tout de même des règles à respecter pour limiter les interférences entre réseaux voisins, et permettre ainsi leur cohabitation. Ces limites sont définies par l'ARCEP, et contrôlées par l'Agence nationale des fréquences (ANF).

La réglementation impose un seuil maximal de Puissance isotrope rayonnée équivalente (PIRE) pour chacun des équipements WiFi déployés. Rappelons que le PIRE est la puissance émise dans l'axe de rayonnement principal d'une antenne (pour plus de détails, voir § 4.4.1). Quand on l'exprime en dBm, le PIRE est égal à la puissance de l'émetteur (en dBm), moins les pertes dans les connecteurs et câbles d'antennes (en dB), plus le gain de l'antenne (en dBi).

Les différentes limites à respecter, selon les canaux utilisés, et selon qu'on déploie le matériel WiFi à l'intérieur ou à l'extérieur sont présentées dans les paragraphes qui suivent.

11.3.2 Limites pour la bande des 2,4 GHz

Ces limites concernent le 802.11b, le 802.11g et le 802.11n lorsqu'il est configuré sur un canal dans la bande des 2,4 GHz.

Canal	Fréquence	PIRE maximal autorisé	
		Intérieur	Extérieur
1 à 7	2 400 à 2 454 MHz	100 mW (20 dBm)	100 mW (20 dBm)
8 à 13	2 454 à 2 483,5 MHz		10 mW (10 dBm)

Exceptions – Dans les départements et collectivités territoriales d'Outremer, le PIRE maximal autorisé est de 100 mW (20 dBm), à l'intérieur comme à l'extérieur des bâtiments.

1. Jusqu'en avril 2007, les opérateurs de *hotspots* WiFi étaient sous un régime expérimental, et n'avaient pas toutes les obligations des opérateurs de réseaux classiques. Désormais, il faut obtenir une licence d'opérateur de *hotspots* si vous souhaitez fournir un service de connexion à Internet pour le grand public. Note : les petits opérateurs (moins d'un million d'euros de chiffre d'affaires annuel) sont exemptés des taxes administratives dues par les opérateurs de réseaux.

11.3.3 Limites pour la bande des 5 GHz

Ces limites concernent le 802.11a et le 802.11n lorsqu'il est configuré sur un canal à 5 GHz.

Canal	Fréquence	PIRE maximal autorisé	
		Intérieur	Extérieur
36 à 48	5 150 à 5 250 MHz	200 mW (~23 dBm)	~ Interdit ~
52 à 64	5 250 à 5 350 MHz	200 mW (~23 dBm) DFS* et TPC**[a]	
100 à 140	5 470 à 5 725 MHz	1 000 mW (30 dBm) DFS* et TPC**	
149 à 161	5 725 à 5 825 MHz	~ Interdit ~	

a. **(*)** – Pour ces fréquences, un mécanisme de sélection dynamique de fréquence (*Dynamic Frequency Selection*, DFS) est obligatoire. La législation précise que ce mécanisme doit respecter la norme harmonisée EN 301 893 de l'ETSI (ou une fonctionnalité équivalente) : « *Ceci doit permettre de garantir au minimum, pour les autres applications autorisées dans la bande concernée, notamment les systèmes de radiolocalisation, un degré de protection identique à celui apporté par la norme harmonisée. Ces techniques d'atténuation égalisent la probabilité de sélection d'un canal spécifique pour tous les canaux disponibles, afin de garantir, en moyenne, une répartition quasi-uniforme de la charge du spectre* ». Les produits 802.11n émettant sur la bande des 5 GHz mettent en œuvre un mécanisme DFS satisfaisant. En ce qui concerne les produits 802.11a, il faut vérifier qu'ils respectent également la norme 802.11h.
(**) – Pour ces fréquences, il faut un mécanisme de contrôle automatique de la puissance de l'émetteur (*Transmitter Power Control*, TPC) permettant d'atteindre une atténuation d'au moins 3 dB. Si un tel mécanisme n'est pas mis en œuvre, le PIRE maximal autorisé est diminué de 3 dB (par exemple, 500 mW au lieu de 1000 mW, c'est-à-dire 27 dBm au lieu de 30 dBm). Là aussi, les produits 802.11n et 802.11a+h mettent en œuvre un mécanisme TPC satisfaisant.

Notons que la réglementation à 5 GHz précise également la densité de PIRE moyenne maximale autorisée. L'objectif est que la puissance rayonnée soit équitablement répartie sur toute la largeur du canal utilisé (large de 20 MHz). Cette limite est égale au PIRE maximal divisé par 20, pour une largeur de bande de 1 MHz. Par exemple, entre 5 470 et 5 725 MHz, la densité de PIRE moyenne maximale autorisée est égale à 1 000/20 = 50 mW/MHz. Les matériels ayant reçu le label WiFi de la WiFi Alliance respectent naturellement cette limite.

11.3.4 Comment respecter ces limites ?

En général, pour respecter la limite de PIRE légale, il n'y a rien à faire de particulier : les équipements WiFi sont en effet le plus souvent équipés d'antennes omnidirectionnelles n'offrant que 2 à 3 dBi de gain, les émetteurs produisent par défaut un signal d'une puissance de 15 à 18 dBm, et la perte dans les connecteurs et câbles d'antenne est proche de 1 à 2 dBm. Ainsi les équipements WiFi vendus en France ont par défaut un PIRE inférieur ou égal à 20 dBm, donc tout à fait dans les limites légales... sauf si l'on installe le point d'accès à l'extérieur sur un canal compris entre 8 et 13 (inclus) : il faut alors réduire la puissance de l'émetteur ou installer un long câble d'antenne ou un atténuateur entre le point d'accès et les antennes (mais le mieux est sans aucun doute de simplement changer de canal).

Les choses sont moins simples si vous modifiez la configuration par défaut, car il faut alors bien faire attention à rester dans la légalité :

- Faites attention si vous réglez la puissance de l'émetteur sur une valeur plus élevée que celle par défaut. Par exemple, vous serez vraisemblablement dans l'illégalité si vous réglez la puissance de l'émetteur à 20 dBm, car on doit rajouter le gain de l'antenne pour calculer le PIRE, et ce dernier risque donc fort de dépasser 20 dBm (à moins d'avoir un long câble d'antenne ou un atténuateur dont les pertes compensent le gain de l'antenne).
- Faites attention également si vous changez le pays pour lequel le point d'accès est configuré : certains pays ont une limite plus élevée que la France et vous risquez donc d'avoir un PIRE très excessif (jusqu'à 30 dBm, c'est-à-dire 10 fois la limite légale).
- Surtout, faites très attention si vous remplacez une antenne[1] par une autre antenne ayant un gain plus important : baissez si nécessaire la puissance de l'émetteur pour respecter la limite de PIRE (voir le chapitre 5).
- Enfin, nous avons malheureusement pu constater que certains installateurs de matériels WiFi sont très peu soucieux de ces limites de PIRE : il n'est pas rare qu'ils installent des antennes directionnelles ou sectorielles à gain important pour améliorer la couverture radio (par exemple en intérieur pour couvrir un bureau situé au bout d'un couloir, ou à l'extérieur pour installer un pont radio), mais sans réduire pour autant la puissance d'émission des points d'accès. Si vous faites appel à un installateur, assurez-vous qu'il respecte bien les limites légales de PIRE.

Bien qu'on entende parfois parler d'un *hotspot* WiFi fermé car il dépassait le PIRE légal, on est obligé de constater que les contrôles sont très rares. Du coup, c'est parfois un peu la « course à l'armement » : un voisin émet trop fort ? Qu'à cela ne tienne, on augmente aussi la puissance de ses équipements ! Il serait pourtant tellement plus simple et efficace d'aller discuter avec ce voisin (et de porter plainte s'il persiste).

On peut également parfois être tenté de « déborder un peu » : 21, 22, 23 dBm, cela semble si proche de 20 dBm... Pourtant n'oubliez pas que 23 dBm, ce n'est pas « un peu plus » que 20 dBm : c'est deux fois plus de puissance rayonnée. C'est un peu comme si vous rouliez à 260 km/h sur l'autoroute ! Évitez donc de dépasser le PIRE légal, même d'un ou deux dBm.

Le fait de bien respecter ces limites permet d'éviter les amendes, de partager respectueusement les ondes avec ses voisins et entre vos propres points d'accès... mais aussi de limiter les risques pour la santé, comme nous allons le voir maintenant.

1. Nous parlons ici des antennes émettrices bien sûr : dans de nombreux matériels WiFi, une antenne est utilisée à l'émission et à la réception, l'autre étant utilisée uniquement en réception. La limite de PIRE est bien sûr une limite à l'émission, donc vous pouvez changer comme bon vous semble l'antenne de réception, cela ne change pas le PIRE.

11.4 GARANTIR LA SÉCURITÉ SANITAIRE

11.4.1 Introduction

La législation est-elle suffisante ?

Les ondes électromagnétiques sont-elles dangereuses pour la santé ? Cette question fait régulièrement la Une des journaux, et alimente de nombreuses conversations. Depuis près d'un siècle on sait bien que les ondes électromagnétiques peuvent être dangereuses pour la santé, et il existe donc depuis longtemps des lois qui encadrent le déploiement des équipements radio. La question n'est donc pas de savoir si les ondes électromagnétiques peuvent être dangereuses pour la santé (la réponse est oui, elles peuvent l'être), mais bien de savoir si la réglementation impose des limites suffisantes pour nous protéger.

Effets thermiques et non thermiques

On distingue deux catégories d'effets nocifs des ondes :

- **Les effets thermiques**, simplement dus à l'échauffement des tissus provoqué par les ondes, sont clairement démontrés depuis de nombreuses années, et la législation actuelle a été définie pour nous en protéger : par exemple, le décret n° 2002-775 définit, pour toute installation électromagnétique, une intensité de champ électrique maximale à ne pas dépasser (nous détaillerons cela plus loin). Certains estiment que ce seuil est beaucoup trop élevé, et surnomment d'ailleurs ce décret « le décret barbecue ».
- **Les effets non thermiques** des ondes électromagnétiques seraient, quant à eux, dus à la perturbation des équilibres subtils en jeu dans divers processus biologiques. Ils pourraient être déclenchés par des champs électromagnétiques d'une intensité beaucoup plus faible que les effets thermiques, et seraient plus complexes et variés... et au moins aussi graves pour la santé. Toutefois, les études se contredisent pour l'instant : certains scientifiques pensent que la preuve est faite qu'ils existent bel et bien, et ils tirent la sonnette d'alarme ; d'autres, au contraire, estiment que ces effets non thermiques n'existent pas, ou en tout cas qu'ils sont si limités qu'ils sont indécelables. Bref, il n'y a pas encore de consensus scientifiques à leur sujet, et l'on ne peut parler qu'au conditionnel pour l'instant.

Autres obligations légales en matière de sécurité sanitaire

Le décret n° 2002-775 n'est pas la seule obligation légale en matière de sécurité sanitaire lorsque l'on déploie un réseau WiFi : il faut évidemment une installation aux normes d'un point de vue électrique (pour éviter les risques d'électrocution et d'incendies) ; si vous installez vos points d'accès dans un avion ou un train, ils doivent respecter des normes très strictes concernant le feu, les fumées, leur résistance aux chocs ; ils doivent être bien fixés, etc. Mais ces obligations ne sont pas spécifiques au WiFi, et nous ne les aborderons donc pas davantage ici.

Commençons donc par les effets thermiques.

11.4.2 Les effets thermiques des ondes

Analogie sonore

On peut comparer les ondes électromagnétiques aux ondes sonores : un son trop fort peut crever vos tympans. À 110 décibels, par exemple, le traumatisme est immédiat et les dommages auditifs irréversibles. C'est pourquoi la loi fixe des seuils : par exemple, dans les concerts amplifiés le niveau sonore ne doit pas dépasser 107 décibels à 1 mètre des enceintes. Est-ce suffisant ? On peut d'une part contester la valeur de cette limite, car elle semble bien trop proche du seuil de dommages irréversibles. Mais on peut aussi reprocher à cette loi de simplifier excessivement la question en ne prenant en compte que la puissance du son, sans prendre en compte d'autres paramètres. Par exemple, on sait que les sons aigus sont plus dangereux pour les tympans que les sons graves. On sait que le bruit répétitif d'un robinet qui goutte, même s'il est extrêmement faible (et ne risque certainement pas d'endommager vos tympans) peut rendre fou. On sait que travailler toute la journée dans un bruit continu ou saccadé, même de puissance modérée, dans une usine par exemple, peut entraîner un stress important, avec les conséquences que cela peut avoir pour la santé. Bref, le bruit peut nuire à une puissance bien inférieure à celle qui pourrait percer vos tympans, et il ne nuit pas qu'aux oreilles. Évidemment, cette analogie avec les ondes sonores ne vise qu'à donner une idée des arguments qui sont avancés en ce qui concerne les ondes électromagnétiques. Revenons donc maintenant au WiFi.

Les brûlures des ondes

De même qu'un son trop fort peut percer les tympans, un rayonnement électromagnétique trop puissant peut entraîner des effets dits « thermiques », plus ou moins sévères selon la puissance du rayonnement reçu par la victime. Pour des rayonnements extrêmement puissants, cela peut aller jusqu'à des brûlures internes et externes, pouvant même entraîner la mort. Pour des rayonnements moins puissants les effets sont similaires à ceux de la fièvre ou de la chaleur : altération de la concentration, de la mémoire, dégradation de diverses fonctions corporelles, telles que le cœur et la circulation sanguine, déficit du système immunitaire, baisse de la fécondité, etc. Certains organes sont particulièrement à risque, comme les yeux par exemple (risque de cataracte). Tous ces effets sont plutôt bien connus, et ils sont étayés par de nombreuses études scientifiques depuis plus de 50 ans.

Le décret n° 2002-775

La législation française, ainsi que la plupart des législations en Europe et dans le monde, repose sur les travaux de la Commission internationale de protection contre les ondes radio non ionisantes (ICNIRP, www.icnirp.de)[1], dont les résultats ont été publiés en 1998. L'ICNIRP est une organisation internationale non gouvernementale qui vise à protéger les populations et l'environnement contre les dangers des émissions

1. Cette commission a été mise en place par l'Association internationale de protection contre les radiations (IRPA, www.irpa.net) qui regroupe des associations de radioprotection un peu partout dans le monde, dont par exemple la Société française de radioprotection (SFRP, www.sfrp.asso.fr).

radio non ionisantes. Un rayonnement électromagnétique est dit « non ionisant » si chaque quantum de rayonnement ne transporte pas assez d'énergie pour ioniser des atomes ou des molécules, c'est-à-dire pour leur arracher des électrons. C'est le cas des rayonnements de fréquence inférieure à 1 000 GHz, dont le WiFi, situé à 2,4 ou 5 GHz[1].

L'ICNIRP est l'organisation officiellement reconnue par l'Organisation mondiale de la santé (OMS, www.who.int) ainsi que par l'Organisation internationale du travail (OIT, www.ilo.org) dans le domaine des rayonnements non ionisants. Le Conseil de l'Union européenne a adopté le 12 juillet 1999 la recommandation 1999/519/CE qui fixe des seuils de puissance destinés à protéger des effets des rayonnements non ionisants, en s'inspirant entièrement de l'approche et des résultats de l'ICNIRP. Les seuils choisis correspondent à un niveau 50 fois inférieur à l'apparition des premiers symptômes observés par l'ICNIRP, afin de se prémunir des effets à long terme. Les réglementations des pays membres résultent donc de la transposition dans leur législation de cette recommandation européenne issue des travaux de l'ICNIRP. En France, c'est le décret n° 2002-775 du 3 mai 2002 qui a introduit ces seuils dans le droit français. Pour les fréquences qui nous intéressent, à 2,4 GHz et 5 GHz, ce décret fixe à 61 Volts par mètre (V/m) l'intensité maximale du champ électrique mesuré à proximité d'un émetteur, à l'exception d'un périmètre de sécurité qui devra être clairement balisé et où seuls des techniciens formés pourront accéder.

Estimer l'intensité du champ électrique

Jusqu'à présent, nous avons parlé de puissance de rayonnement et non d'intensité de champ électrique. Heureusement, il existe une formule assez simple qui permet d'estimer approximativement l'intensité du champ électrique que l'on pourra mesurer à une distance donnée d'un émetteur WiFi en fonction de son PIRE, si l'on se place dans l'axe de l'antenne. L'intensité du champ électrique est notée E et se mesure en Volts par mètre, la distance d se mesure en mètres, et le PIRE en Watts (pour convertir une puissance exprimée en dBm en Watts, voir § 2.2.1). Voici cette formule :

$$E = 5{,}5 \times \frac{\sqrt{PIRE}}{d}$$

Comme nous l'avons vu au § 11.3, le PIRE maximal autorisé en France à 2,4 GHz est fixé à 20 dBm, donc 100 mW, c'est-à-dire 0,1 W. Si l'on se place à 3 mètres d'un point d'accès réglé à pleine puissance, le niveau du champ électrique devrait se situer aux alentours de :

$$E = 5{,}5 \times \frac{\sqrt{0{,}1}}{3} \approx 0{,}58\ V/m$$

À 3 mètres d'un AP WiFi à 2,4 GHz émettant à pleine puissance, le champ électrique est donc environ 100 fois inférieur à la limite légale de 61 V/m, elle-même

1. Les rayonnements ionisants (ultraviolets, rayons X, rayons gammas...) sont, quant à eux, particulièrement dangereux et font l'objet d'une législation tout à fait distincte.

50 fois inférieure à la limite d'apparition des premiers symptômes thermiques, selon les résultats de l'ICNIRP.

À l'inverse, pour connaître la distance minimale à laquelle on doit se placer d'un AP WiFi (ou plus exactement de ses antennes) émettant à pleine puissance si l'on souhaite respecter la limite imposée par le décret n° 2002-775, on applique la formule suivante :

$$d_{min} = 5{,}5 \times \frac{\sqrt{PIRE_{\max}}}{E_{\max}}$$

Pour le WiFi à 2,4 GHz, on a $PIRE_{max}$ = 0,1 W et E_{max} = 61 V/m, donc le calcul donne $d_{min} \approx 2{,}8$ cm.

Pour respecter le décret n° 2002-775, il faut donc se placer à plus de 3 cm environ des antennes d'un AP émettant à 100 mW, c'est-à-dire à pleine puissance pour la bande de 2,4 GHz. À 5 GHz, le PIRE maximal est égal à 1 Watt, et le calcul montre qu'il faut alors se placer à plus de 9 cm.

Si l'on fait confiance aux seuils fixés par le décret de 2002, on ne devrait pas avoir de souci à se faire au sujet des points d'accès, car on ne les installe jamais à moins de 10 cm des utilisateurs. Mais attention : les points d'accès ne sont pas les seuls à émettre, un ordinateur portable peut lui aussi théoriquement émettre à 100 mW à pleine puissance (dans la pratique, plutôt la moitié), et beaucoup de gens posent leur ordinateur sur leurs genoux.

Le décret n° 2003-961

On peut surtout s'interroger sur les téléphones WiFi : s'ils émettent à pleine puissance, la tête de l'utilisateur se trouve à l'intérieur du périmètre limite calculé plus haut. D'ailleurs, en admettant que le téléphone WiFi soit placé contre l'oreille, donc mettons à 0,5 cm du crâne, alors l'intensité du champ électrique dans lequel baigne la partie du crâne contre laquelle s'appuie le téléphone est d'environ... 350 V/m à 100 mW ($PIRE_{max}$ à 2,4 GHz), et 1 100 V/m à 1 W ($PIRE_{max}$ à 5 GHz), soit respectivement 5,7 fois et 18 fois plus que la limite fixée par le décret. Cela reste inférieur au seuil à partir duquel des symptômes thermiques ont pu être observés (rappelons-le, 50 fois la limite fixée par le décret), mais il n'empêche que le seuil de sécurité fixé par le décret de 2002 est largement dépassé.

Toutefois le décret de 2002 ne s'applique qu'aux installations électromagnétiques (les points d'accès). Pour les terminaux, tels que les téléphones WiFi, c'est le décret n° 2003-961 du 8 octobre 2003 qui s'applique (également issu des travaux de l'ICNIRP). La puissance émise par un terminal, émettant au maximum d'intensité et dans les pires conditions d'utilisation, sera en partie absorbée par le corps humain. Cette puissance réellement absorbée se mesure en Watt par kilogramme de tissu (W/kg): c'est ce qu'on appelle le Débit d'absorption spécifique (DAS). Le décret de 2003 fixe le DAS maximal à 2 W/kg moyenné sur 10 grammes de tissu, au niveau du tronc et de la tête (on parle de « DAS local »). En outre, le terminal ne doit pas exposer l'utilisateur à plus de 0,08 W/kg moyenné sur l'ensemble du corps (c'est le « DAS global »). Aujourd'hui, la plupart des téléphones portables GSM commercialisés en

Europe ont un indice compris entre 0,4 et 1,4 W/kg moyenné sur 10 grammes, et les téléphones WiFi ont un DAS du même ordre. Par exemple, l'iPhone 3G d'Apple, lorsqu'il est configuré en mode WiFi, a un DAS (au niveau de la tête) environ égal à 0,371 W/kg, alors que l'indice atteint 0,878 W/kg en mode 3G, et 0,780 W/kg en GSM à 1 800 MHz, mais seulement 0,235 W/kg en mode GSM à 900 MHz.

Les téléphones WiFi respectent donc bien le décret de 2003. Néanmoins, par précaution, on peut conseiller de limiter l'utilisation des téléphones portables (WiFi, DECT ou GSM) par les jeunes enfants, d'utiliser des oreillettes et d'éviter de téléphoner pendant trop longtemps.

On fait souvent remarquer qu'un téléphone WiFi rayonne généralement à une puissance de 100 mW tandis qu'un téléphone portable GSM émet jusqu'à 2 W, soit 20 fois plus. On ne peut toutefois pas comparer aussi simplement les téléphones GSM et les téléphones WiFi : en effet, contrairement aux téléphones mobiles GSM, les équipements WiFi n'ont généralement pas de système d'adaptation dynamique de la puissance. Avec un téléphone mobile GSM, la puissance d'émission est réduite lorsque le niveau de réception du signal de l'antenne relais est bon, et inversement, il augmente lorsque les conditions de réception sont mauvaises : c'est pourquoi l'on déconseille souvent de téléphoner dans un ascenseur, dans un train, ou en déplacement. Au contraire, la plupart des téléphones WiFi émettront toujours à la puissance maximale dont ils sont capables (jusqu'à 0,1 W à 2,4 GHz, et théoriquement jusqu'à 1 W à 5 GHz). En outre, le GSM utilise une fréquence plus faible que le WiFi (0,9 GHz ou 1,8 GHz), donc transporte moins d'énergie (ils ont un DAS du même ordre, comme nous l'avons vu).

Des effets thermiques très limités

Si l'on en croit les travaux de l'ICNIRP sur lesquels reposent les décrets de 2002 et 2003, le risque des effets thermiques des ondes non ionisantes provient exclusivement des terminaux WiFi collés contre le corps pendant une période prolongée. Ceci est vrai pour le WiFi, le GSM, le DECT, le Wimax, etc. Donc lorsque vous déployez des points d'accès WiFi, pour limiter les risques dus aux effets thermiques des ondes, il suffit de vous assurer que vous respectez bien les limites de PIRE que nous avons vus au § 11.3, et que vous installez ces AP à bonne distance des utilisateurs (dans les faux plafonds par exemple). Sauf si les effets non thermiques s'en mêlent...

11.4.3 Les effets non thermiques

Presque tout le monde semble d'accord pour estimer que les effets thermiques des ondes sont très limités ou nuls dans le cas du WiFi (vue la faible puissance d'émission). L'essentiel du débat porte en réalité sur la question suivante : les rayonnements non ionisants ont-ils d'autres effets nocifs que leurs effets thermiques ? Si oui, ces effets peuvent-ils survenir avec un champ électrique d'une intensité inférieure aux seuils légaux actuels ?

Pour l'instant, nous l'avons dit, il n'y a pas de consensus scientifique sur cette question : la plupart des études sur le sujet ne parviennent pas à démontrer l'existence

d'effets non-thermiques, tandis qu'une minorité d'entre elles concluent à l'existence d'effets potentiellement nocifs à des seuils très inférieurs à ceux imposés par la loi. Mais évidemment, en Science, comme ailleurs, la majorité n'a pas toujours raison.

Des pathologies très nombreuses

Parmi les effets non-thermiques considérés jusqu'à présent, on peut noter (d'après l'association *Les Robins des Toits*[1]) :

- la perte d'étanchéité de la barrière sang-cerveau ;
- la perturbation de production de la mélatonine ;
- la déstabilisation des régulations membranaires ;
- des dommages génétiques.

Ces effets pourraient eux-mêmes déclencher une liste impressionnante de pathologies : cancers, syndromes cardiaques, diverses pathologies cérébrales et psychiques (insomnies, anorexie, stress, dépression...), déficit immunitaire, infertilité, et même des pathologies dermatologiques (rougeurs, irruptions cutanées...), des allergies... et la liste continue encore.

L'électro-sensibilité

Certaines personnes (on parle de 3 % de la population), seraient même « électro-sensibles », c'est-à-dire particulièrement sensibles aux ondes électromagnétiques : elles souffrent de maux de tête, elles ont des sensations de brûlures, des irruptions cutanées, etc. Leur souffrance n'est pas au conditionnel : elle est bien réelle et cette maladie a d'ailleurs été officiellement reconnue dans plusieurs pays. Mais le lien de cause à effet n'est pas (encore ?) établi. Du point de vue de ces personnes électro-sensibles, le lien entre les ondes et leur souffrance est pourtant évident : elles disent par exemple ressentir immédiatement la présence d'un point d'accès WiFi en rentrant dans une pièce, et elles se sentent immédiatement soulagées lorsque l'on éteint ce point d'accès. Toutefois, une étude en double-aveugle menée par l'OMS n'a pas permis de démontrer de corrélation entre la présence d'ondes et les symptômes : on observait parfois des symptômes en l'absence de champ électromagnétique, et *vice versa*. La conclusion de l'étude est que ces symptômes ont vraisemblablement d'autres origines que les ondes (pas forcément psychosomatiques d'ailleurs, contrairement à ce que certains disent) : cela pourrait être dû à une mauvaise luminosité dans le lieu de travail, des écrans d'ordinateurs mal réglés, une mauvaise aération ou climatisation, un environnement de travail stressant, etc. Mais là encore, il n'y a pas de consensus scientifique.

1. Le dossier scientifique disponible sur le site web de cette association est très complet et nous vous invitons à le consulter pour plus de détails. Attention : les études présentées sont bien sûr presque exclusivement des études qui concluent qu'il existe un risque. Pour ne pas vous limiter à un seul point de vue, consultez également le site web de l'ANF ou de l'OMS, par exemple.

Les ondes pulsées

Les ondes électromagnétiques sont bien étudiées depuis longtemps, et la bande de fréquences de 2,4 GHz l'est particulièrement depuis l'apparition, il y a plus de 20 ans, des fours à micro-ondes qui fonctionnent justement sur cette bande de fréquences. Qu'y a-t-il donc de nouveau avec le WiFi, le GSM ou encore le Wimax ? La différence viendrait de la structure de l'onde : alors que le four à micro-ondes émet une onde simple, le WiFi émet une onde complexe qui se décompose en une onde à haute fréquence, et des ondes très saccadées, à basses fréquences (on parle d'ondes « pulsées »). Ce sont ces saccades qui perturberaient le plus les processus biologiques, et seraient donc particulièrement nocives.

La difficulté de la preuve

Au premier abord, la question semble plutôt simple à trancher : existe-t-il, oui ou non, des effets nocifs non thermiques ? Pourtant, force est de constater qu'après des années d'étude, l'incertitude demeure. Pour ceux qui voudraient démontrer l'absence de risque, la difficulté est fondamentale. En effet, ils ne pourront jamais conclure autre chose que ceci : « *sur tous les cas que nous avons étudiés, nous n'avons pas observé de pathologie due aux ondes* ». On pourra donc toujours leur répondre : « c'*est que vous n'avez pas étudié assez de cas, ou pendant pas assez longtemps car les effets peuvent survenir après plusieurs années* ». Démontrer l'absence de risque est impossible : tout au plus on peut augmenter, étude après étude, le degré de confiance. Exiger la preuve absolue de l'absence de risque est donc absurde.

Mais à l'inverse, démontrer l'existence d'un risque n'est pas forcément aisé non plus. Souvenons-nous qu'il a fallu des décennies pour pouvoir démontrer que la cigarette provoquait bien des cancers ! Il ne suffit pas de trouver une personne malade, encore faut-il parvenir à démontrer que sa maladie provient bien des ondes. Et pour pouvoir quantifier le risque, un seul malade ne suffit pas : il en faut beaucoup. C'est précisément l'intérêt des études épidémiologiques : elles concernent des populations entières. La plus grande étude épidémiologique menée jusqu'à présent au sujet des effets des ondes s'appelle *Interphone*. Il s'agit d'une étude menée à l'échelle européenne : des milliers de personnes ont rempli des questionnaires, en indiquant notamment leur fréquence d'utilisation du téléphone portable, ainsi que des informations sur leur état de santé. Des résultats intermédiaires ont été publiés dans certains pays, et ils faisaient apparaître un taux de cancer du cerveau beaucoup plus important chez les gros utilisateurs de téléphones portables. Les journalistes se sont évidemment emparés du scoop. Mais c'est oublier que ces résultats sont bruts et purement déclaratifs : or, une personne atteinte d'un cancer du cerveau a semble-t-il tendance à attribuer sa maladie au téléphone portable, et en conséquence à se déclarer « gros utilisateur », alors qu'elle ne l'est pas forcément plus que les autres. C'est pourquoi l'étude *Interphone* prévoit dans un deuxième temps que les factures téléphoniques d'un échantillon de personnes soient épluchées afin de pouvoir « calibrer » les réponses subjectives. Cela donne une idée de la difficulté qu'il y a à mener une étude épidémiologique dont les résultats soient incontestables (et le danger de divulguer des résultats bruts et partiels). Quoi qu'il en soit les résultats de l'étude *Interphone* sont attendus pour septembre 2009.

Le principe de précaution

Ceux qui réclament l'application du principe de précaution demandent au minimum l'abaissement du seuil de 61 V/m défini par la loi. Certains pays ont d'ores et déjà appliqué ce principe de précaution, au moins dans une certaine mesure. Par exemple, la Suisse fixe le seuil à 3 V/m (soit 20 fois moins) dans les lieux « sensibles », c'est-à-dire fréquentés régulièrement (le seuil reste toutefois égal à 61 V/m pour les endroits peu fréquentés). Certains réclament un seuil encore plus faible, à 0,6 V/m, soit un seuil 100 fois moins élevé qu'actuellement. Ce seuil de 0,6 V/m est en effet préconisé par certaines études.

Dans le cas du WiFi, si l'on émet à 100 mW, cela signifie qu'il faut installer les points d'accès à plus de 3 mètres des utilisateurs. Ce n'est pas impossible, mais cela complique évidemment le déploiement. L'autre solution consiste à réduire la puissance des points d'accès. Par exemple, en réduisant la puissance à 10 dBm (au lieu de 20 dBm), c'est-à-dire 10 mW (au lieu de 100 mW), il suffit de garantir un périmètre de sécurité d'un mètre environ autour de chaque point d'accès. En émettant moins fort, on a une couverture moindre, et donc pour éviter les trous de couverture, on est obligé d'installer plus de point d'accès, plus rapprochés les uns des autres. Cela peut paraître paradoxal : pour un environnement radio plus sûr, il faut des points d'accès moins puissants... mais du coup plus nombreux.

11.4.4 Un débat passionné

Des autorités très rassurantes

Du point de vue des autorités sanitaires françaises, les choses sont plutôt simples : le WiFi ne pose aucun risque pour la santé, pourvu que l'on respecte les limites légales de PIRE que nous avons présentées au § 11.3. L'Agence française de sécurité sanitaire de l'environnement et du travail (AFSSET) affirme que « *malgré un très grand nombre d'études réalisées aussi bien sur des cultures cellulaires in vitro que sur des animaux in vivo depuis plusieurs années, les chercheurs n'ont pu prouver l'existence de manière sûre et reproductible d'effets qui ne seraient pas dus à un échauffement créé par l'absorption des micro-ondes, et qui posséderaient un réel impact sanitaire* ». De son côté, la Fondation santé et radiofréquences affirme que « *les études menées jusqu'à aujourd'hui n'ont permis d'identifier aucun impact des radiofréquences sur la santé en deçà [des limites légales]* ». L'école Supélec a publié une étude fin 2006 qui concluait que, même en disposant plusieurs émetteurs WiFi à proximité les uns des autres, on n'observe pas d'effet cumulatif significatif (car la puissance diminue avec le carré de la distance, donc la puissance observée en un point provient essentiellement de l'émetteur le plus proche), et l'on reste en tout point bien en dessous des limites définies par le décret n° 2002-775.

Au niveau international aussi, on a généralement le même son de cloche : l'Agence de protection de la santé au Royaume-Uni précise qu'une personne assise à proximité d'un *hotspot* WiFi pendant un an reçoit la même dose d'ondes qu'une personne qui utilise son téléphone portable pendant 20 minutes. Enfin, l'OMS soutient également

que le WiFi ne devrait susciter aucune inquiétude (mais propose tout de même quelques mesures de précaution, à titre préventif).

Des associations tirent la sonnette d'alarme

De leur côté, un certain nombre de scientifiques ainsi que plusieurs associations militent pour que la question de la dangerosité des ondes soit prise plus au sérieux. En France, citons par exemple les associations *Les Robins des Toits*, *Agir pour l'Environnement* ou encore *Priartem*. Ces associations soulignent que plusieurs études scientifiques concluent à la dangerosité des ondes (surtout au sujet des téléphones portables et des antennes relais GSM, mais aussi au sujet du WiFi), et donc même si la majorité des études ne parviennent pas à la même conclusion, ces associations estiment que le doute est suffisant pour que les autorités appliquent le principe de précaution, au moins en abaissant très fortement les seuils légaux de puissance de rayonnement. Devant l'insistance de ces associations et la montée de l'inquiétude au sein de la population, le gouvernement français a organisé un « Grenelle des ondes » en avril 2009. Celui-ci n'a pas satisfait les associations dont plusieurs ont claqué la porte après quelques semaines de discussion, estimant qu'il n'y avait aucune avancée sérieuse. En ce qui concerne le WiFi, ce Grenelle des ondes a simplement conclu que, par mesure de précaution, les installations WiFi devaient être évitées à proximité des jeunes enfants, et notamment dans les crèches, les écoles primaires et les maternelles.

Un débat qui s'envenime

Les opinions sur ce sujet sont souvent très tranchées : dans les articles et les forums, on lit fréquemment des termes assez brutaux de part et d'autre : en caricaturant à peine, il y a d'un côté les « anti-ondes », qui parlent de « pollution électromagnétique » et accusent le « lobby des opérateurs » d'amasser des milliards d'euros au détriment de la santé publique, pendant que des « politiciens irresponsables » ferment les yeux, voire même touchent leur chèque ; et de l'autre côté, il y a les « pro-ondes », qui estiment que les craintes des « anti-ondes » ne sont que « pure paranoïa », les personnes électrosensibles ne seraient que des « affabulatrices », toutes les craintes ne seraient que « fantasme » entretenu par des médias intéressés uniquement à « vendre de la peur » et par des vendeurs de « grigris » (peintures, tissus, patchs destinés à protéger des ondes).

Les raisons de la passion

Est-il donc possible d'avoir un débat posé à ce sujet ? Pourquoi cette passion ? En premier lieu bien sûr car il s'agit d'une question qui touche à la santé : quoi de plus naturel que de se soucier de sa santé et de celle de ses proches ? Ensuite, c'est un sujet pour lequel, nous l'avons vu, il n'y a pas encore de consensus scientifique. Chacun peut donc brandir l'étude dont la conclusion va dans le sens qui lui convient et déclarer que la preuve est faite. Mais il y a encore bien d'autres raisons.

Plusieurs affaires ont entaché la réputation des opérateurs, et la méfiance à leur égard est donc grande en France[1]. En 2005, les trois opérateurs mobiles français, Orange, SFR et Bouygues Télécom ont été condamnés à payer plus d'un demi-milliard d'euros d'amende pour s'être entendus sur leurs tarifs, en violant les règles élémentaires de la concurrence, au détriment du consommateur. Cette amende historique ne représente pourtant même pas un mois de leur chiffre d'affaires. Rajoutez à cela une tarification incompréhensible, un service client délocalisé, injoignable et au prix prohibitif (depuis 2008 ceci est toutefois mieux réglementé), un service de qualité médiocre (comparé au service filaire), des « zones blanches » sans service car non rentables, etc. Bref, pour beaucoup de Français, les opérateurs sont des escrocs : s'ils prétendent que les ondes sont sans danger, ou si des études qu'ils ont financées (même en partie) l'affirment, alors cela n'a aucune valeur, c'est même suspect.

De même, plusieurs affaires ont terni la réputation des autorités sanitaires : la catastrophe de Tchernobyl, l'affaire du sang contaminé, l'amiante, autant de sujets sur lesquels les autorités ont gravement manqué de transparence. Bien sûr, on peut répondre à cela qu'il est difficile d'être parfaitement transparent sans risquer la panique (qui peut être pire que le mal). En outre, livrer des informations brutes, souvent techniques, à un public non averti peut entraîner des confusions inutiles (on l'a vu plus haut avec l'étude *Interphone*). Mais ces arguments ne feront pas oublier des catastrophes comme Tchernobyl : la plupart des Français exigent désormais d'être informés en direct et en toute transparence. Autre motif de désamour entre les Français et les autorités sur les questions sanitaires : le manque de concertation sur certains sujets importants, tels que le développement du nucléaire ou les OGM (que l'on soit favorable ou non à ces technologies). Avec tous ces éléments en tête, on comprend mieux pourquoi de nombreux Français n'accordent que peu de valeur aux paroles rassurantes des autorités concernant les ondes électromagnétiques.

Le concept même d'un « principe de précaution » ne fait pas l'unanimité. Certains voient ce principe comme une évidence : on ne devrait rien faire qui puisse mettre des vies en danger, et l'on ne doit pas attendre d'être sûr avant d'agir pour éviter des catastrophes (on pense au réchauffement de la planète par exemple). D'autres estiment que ce principe inhibe toute action : si l'on refuse tout risque, on ne fait plus rien. D'autres encore pensent que le principe de précaution peut lui-même être dangereux : par exemple, certains pesticides ont été brutalement interdits dans certains pays lorsqu'on a constaté qu'ils étaient dangereux pour la santé, en application du principe de précaution. Dans plusieurs de ces pays (notamment en Amérique du Sud), les moustiques ont alors proliféré rapidement, et la recrudescence de malaria a provoqué bien plus de morts que les pesticides eux-mêmes. Certains estiment enfin que le principe de précaution tend à accroître les inégalités entre les pays riches et les pays pauvres, en imposant des solutions plus sûres mais plus coûteuses.

La passion autour de ce sujet incite bel et bien les journalistes à s'y pencher de près, que ce soit pour « vendre du papier » ou par « conscience citoyenne », selon votre

1. Il est d'ailleurs frappant de constater que, dans la version française de la Wikipedia, l'article sur le WiFi parle longuement de la santé, alors que dans la version anglaise, le sujet n'est même pas abordé.

vision des choses. En retour, cette médiatisation importante stimule l'intérêt et les passions autour de ce sujet : c'est donc un cercle vicieux ou vertueux, une « paranoïa collective » ou « prise de conscience salvatrice »... selon votre vision des choses.

On l'aura compris, le débat va bien plus loin que la question stricte des ondes électromagnétiques : il est question de mode de vie, de vision de la société, de politique. Il n'est pas rare de lire des arguments du type « *la voiture pollue et fait des milliers de morts par an, et pourtant elle n'est pas interdite, pourquoi interdirait-on le WiFi ? Allons de l'avant !* », ou inversement « *nous devons rejeter le WiFi, même s'il n'est pas dangereux pour la santé, car il contribue à nous isoler les uns des autres, il encourage notre glissement vers une société ultra-technologique, totalement déshumanisée* ».

Faites-vous votre idée

La question purement scientifique de l'effet sur la santé des ondes électromagnétiques est donc mêlée à de nombreuses autres considérations, et il est bien difficile de distinguer les faits des opinions.

C'est pourquoi, nous ne pouvons que vous inviter à vous faire votre propre opinion en consultant les divers points de vue : vous trouverez de nombreuses études sur les effets non thermiques des ondes sur le site web de l'association *Les Robins des Toits* ; consultez également le site web de l'OMS ainsi que l'ANF, qui ont chacun créé un dossier sur la question de l'effet des ondes sur la santé.

Glossaire

1G La téléphonie mobile de 1re génération est analogique. Elle n'est pas conçue pour l'échange de données.

2G La téléphonie mobile de 2e génération est numérique et bien plus performante que la 1G. Exemples : GSM, CDMA, CDPD...

2,5G Des technologies telles que le GPRS ou l'EDGE ont été conçues pour permettre la navigation sur Internet ou encore l'échange de contenu multimédia en reposant sur les réseaux de la 2G. On appelle ceci la téléphonie de génération « deux et demi ».

3G La troisième génération de téléphonie vise des débits bien supérieurs à la 2,5G et aspire à l'universalité. Exemples : UMTS, CDMA2000...

802.1D Norme de l'IEEE pour les ponts de réseaux locaux.

802.1Q Norme de l'IEEE pour les réseaux virtuels (VLAN).

802.1x Norme de l'IEEE pour le contrôle d'accès à un réseau. Le contrôle est exercé au niveau d'un port d'un commutateur, ou pour chaque association dans un AP. Ce standard repose sur l'EAP et l'authentification des utilisateurs est généralement réalisée par un serveur RADIUS.

802.2 Norme de l'IEEE définissant la couche réseau LLC.

802.3 Norme de l'IEEE pour les réseaux locaux filaires, inspiré d'Ethernet.

802.3af Norme de l'IEEE pour le PoE.

802.11 Norme conçue par l'IEEE en 1997 pour les réseaux locaux sans fil et constamment améliorée depuis. Elle définit trois couches physiques (infrarouge, FHSS et DSSS sur les fréquences de 2,4 GHz) et une couche MAC offrant de nombreuses fonctionnalités : partage du média, fragmentation, économie d'énergie, sécurité...

802.11a Amélioration du 802.11 sur les fréquences de 5 GHz. Grâce à la modulation radio OFDM, cette variante du WiFi peut atteindre un débit théorique de 54 Mb/s.

802.11b Amélioration du 802.11 DSSS, cette variante du WiFi peut atteindre un débit théorique de 11 Mb/s grâce à la modulation radio HR-DSSS.

802.11c Précisions destinées aux constructeurs d'AP (pour le mode bridge).

802.11d Précisions pour les constructeurs de matériel WiFi (internationalisation).

802.11e Amélioration de la couche MAC du 802.11, destinée à permettre une meilleure gestion de la QoS.

802.11F Définit l'IAPP.

802.11g Amélioration du 802.11b : elle peut atteindre 54 Mb/s grâce à la modulation radio OFDM.

802.11h Adaptation du 802.11a à la législation européenne, grâce au TPC et au DFS.

802.11i Nouvelle norme de sécurité pour le 802.11, en remplacement du WEP. Voir WPA.

802.11j Adaptation du 802.11 à la législation japonaise.

802.11k Amélioration du 802.11 pour faciliter les mesures radio.

802.11legacy Nom donné à la première version du standard 802.11, publié en 1997. Voir 802.11.

802.11m Groupe de travail du 802.11 chargé de la maintenance de la norme.

802.11n Dernière amélioration en date de la couche physique du 802.11, le 802.11n permet d'atteindre 600 Mb/s, grâce à la technique radio MIMO, à l'utilisation de bandes de fréquences plus larges et à quelques optimisations de la couche MAC. Il peut être utilisé à 2,4 GHz ou à 5 GHz.

802.11s Groupe de travail pour les réseaux WiFi maillés.

802.15 Norme de l'IEEE pour les WPAN (Bluetooth, UWB, ZigBee...).

802.16 Norme de l'IEEE pour les WMAN (WiMAX).

A

AAA Un serveur AAA (*Autorisation, Authentification, Accounting*) gère l'authentification des utilisateurs, leurs autorisations et la comptabilisation de leurs connexions. Voir aussi RADIUS.

Ad Hoc Dans un réseau WiFi de type Ad Hoc, les stations communiquent directement entre elles plutôt que par le biais d'un AP. Voir aussi Infrastructure.

AES *Advanced Encryption Standard*. Algorithme de cryptage symétrique extrêmement rapide et sûr. La norme de sécurité WPA2 repose sur le TKIP ou l'AES.

AFSSET Agence française de sécurité sanitaire de l'environnement et du travail.

AM *Amplitude Modulation*. Technique radio consistant à « moduler » l'amplitude du signal émis (la « porteuse ») en fonction du signal « source ».

ANF Agence nationale des fréquences. En charge du contrôle de l'utilisation des fréquences radio en France.

AP *Access Point* (point d'accès). Borne WiFi composant l'ossature d'un réseau sans fil. En mode Infrastructure, tout utilisateur doit passer par un AP pour accéder au réseau sans fil : tout son trafic est alors relayé par l'AP auquel il est « associé ».

ARCEP Autorité de régulation des communications électroniques et des postes. Organisme gouvernemental français chargé de réglementer les télécommunications et notamment le WiFi (anciennement appelée ART).

ART Autorité de régulation des télécommunications. Voir ARCEP.

ASK *Amplitude Shift Keying. Modulation*. Radio numérique basée sur l'AM.

ATIM Annonce TIM. Dans un réseau Ad Hoc, message envoyé par une station à une autre station en mode d'économie d'énergie, pour la prévenir qu'elle souhaite lui envoyer un paquet et qu'elle ne doit donc pas se mettre en sommeil.

B

BER *Bit Error Rate*. Proportion de bits mal transmis. Voir aussi FER.

BLR Boucle locale radio. Ensemble de technologies permettant de relier par les ondes radio un abonné à un opérateur (téléphonie, Internet...). Parmi les technologies de BLR les plus utilisées, on compte le LMDS, le MMDS et le WiMAX.

Broadcast Trafic réseau adressé à tout le monde. Voir aussi Multicast et Unicast.

BSS *Basic Service Set*. Un réseau WiFi composé d'un seul AP.

BSSID Identifiant d'un BSS. Il s'agit d'un nombre de 48 bits, égal à l'adresse MAC de l'AP en mode Infrastructure, ou aléatoire en mode Ad Hoc.

C

CAM *Continuously Aware Mode*. Mode sans économie d'énergie. Voir PSM.

CBC *Cipher Block Chaining*. Algorithme produisant un MIC à partir d'un message, en utilisant un algorithme de cryptage par bloc. Le CBC est utilisé par le WPA/AES. Le CBC est souvent appelé le CBC-MAC (*CBC-Message Authentication Code*).

CCK *Complementary Code Keying*. Modulation radio utilisée par le HR-DSSS.

CCM *Counter-Mode with CBC-MAC*. Mode d'utilisation d'un algorithme de cryptage par bloc (ex. AES), mêlant le Counter-Mode (CM) et le CBC.

CCMP *CCM Protocol*. Protocole pour le 802.11i sur AES (WPA2).

Cellule Zone couverte par le signal d'un point d'accès WiFi. Voir aussi BSS.

CFP *Contention Free Period*. Période de partage d'un média sans risque de collision. Les modes PCF et EPCF définissent une période CFP entre chaque balise.

Chipping Technique consistant à émettre plusieurs bits (appelés des « *chips* ») pour chaque bit d'information à envoyer. Grâce à la redondance du signal émis, les erreurs de transmission peuvent être réduites. Par ailleurs le spectre radio du signal émis est ainsi étalé, ce qui permet d'atteindre un débit plus élevé et de mieux résister au bruit. Voir aussi DSSS.

CM *Counter-Mode*. Mode d'utilisation d'un algorithme de cryptage par bloc tel que l'algorithme AES. Le CM résulte en un algorithme de cryptage par flux.

CNCIS Commission nationale de contrôle des interceptions de sécurité.

CNIL Commission nationale de l'informatique et des libertés.

COFDM *Coded OFDM*. Modulation OFDM renforcée par des codes « convolutifs », correcteurs d'erreur, ce qui assure une meilleure résistance aux interférences.

Collision On parle de « collision » lorsque deux stations émettent un paquet en même temps : généralement, les deux paquets sont alors perdus. Voir aussi CSMA.

CPL Courant porteur en ligne. Technologie permettant de transmettre des données par le biais de l'installation électrique d'un bâtiment (ex. : produits HomePlug).

CRC Code de redondance cyclique. Code d'intégrité assez simple. Voir aussi MIC.

CSMA *Carrier Sense Multiple Access*. Stratégie de partage d'un média très simple : chaque station vérifie que le média soit libre pendant une durée minimale plus un temps aléatoire avant d'émettre un paquet. Ceci permet de limiter les collisions.

CSMA/CA *CSMA with Collision Avoidance*. Variante du CSMA utilisée notamment par les modes DCF et EDCF du WiFi : le récepteur envoie un accusé de réception (ACK) pour chaque paquet reçu : les collisions peuvent ainsi être détectées a posteriori et les paquets concernés peuvent être réémis.

CSMA/CD *CSMA with Collision Detection*. Variante du CSMA utilisée notamment par l'Ethernet. Chaque station écoute le média pendant qu'elle émet un paquet et peut ainsi détecter si une autre station émet un paquet en même temps (collision).

CTS *Clear To Send*. Voir RTS/CTS.

CW *Collision Window* (ou *Contention Window*). Durée maximale de l'attente aléatoire d'une station avant l'émission d'un paquet en mode CSMA.

D

DAS Le débit d'absorption spécifique d'un terminal radio mesure la puissance radio absorbée par les tissus du corps humain (en Watt par kilogramme), dans les pires conditions d'utilisation.

DCF *Distributed Coordination Function*. Stratégie de partage des ondes employée par défaut en WiFi : elle repose sur le CSMA/CA et le mécanisme RTS/CTS.

DFS *Dynamic Frequency Selection*. Sélection automatique d'une fréquence libre.

DoS *Denial of Service*. Une attaque de déni de service consiste à empêcher les utilisateurs d'accéder aux services du réseau. Le WiFi est particulièrement vulnérable aux attaques DoS.

DPSK *Differential PSK*. Modulation numérique où les bits d'information sont codés sous la forme de variations de la phase de l'onde porteuse. Voir aussi PM.

DS *Distribution System*. Il s'agit du lien entre les AP d'un réseau WiFi de type Infrastructure. Généralement le DS est le réseau filaire auquel sont reliés les AP, mais il peut également s'agir d'un lien sans fil. Voir aussi WDS.

DSSS *Direct Sequence Spread Spectrum*. Modulation radio utilisée par le 802.11b et le 802.11g. Grâce à la technique de chipping, le spectre radio occupé par le signal est étalé, ce qui permet d'atteindre des débits plus élevés et de mieux résister au bruit.

DTIM *Delivery TIM*. Envoyé par l'AP dans certaines balises (généralement une sur trois), le DTIM indique aux stations la période pendant laquelle l'AP leur transmettra le traffic broadcast et multicast. Cela permet aux stations en mode d'économie d'énergie de ne pas se mettre en sommeil pendant ces transmissions.

E

EAP *Extensible Authentication Protocol*. Protocole très générique permettant l'identification d'utilisateurs selon diverses méthodes (mot de passe, certificat, carte à puce...). Normalisé par l'IETF comme extension du protocole PPP, l'EAP est maintenant également à la base du 802.1x, lui-même à la base du WPA Enterprise.

EAPoL *EAP over LAN*. Protocole défini par l'IEEE pour le 802.1x. Il permet l'échange de paquets EAP sur un réseau local (LAN).

ECB *Electronic Code Book*. Mode d'utilisation très simple d'un algorithme de cryptage par bloc : le message est découpé en blocs, cryptés indépendamment.

EDCA *Enhanced Distribution Channel Access*. Voir EDCF.

EDCF *Enhanced DCF*. Amélioration du DCF définie dans le 802.11e, ce mode de partage des ondes permet de distinguer des classes de trafic (TC) : le trafic de haute priorité aura plus de chances d'être émis rapidement que le trafic de basse priorité.

EPCF *Enhanced PCF*. Amélioration du PCF définie dans le 802.11e, ce mode de partage des ondes permet de distinguer des classes de trafic (TC). Chaque classe a sa propre QoS, très précise : débit maximal, priorité, fluidité, etc.

ESS *Extended Service Set*. Réseau WiFi de type Infrastructure, pouvant être composé de plusieurs BSS.

ESSID Identifiant d'un ESS, souvent noté simplement « SSID ». Il s'agit d'un nom composé au maximum de 32 caractères.

ETSI *European Telecommunications Standards Institute*. Institut européen des normes de télécommunication, similaire à l'IEEE.

F

FER *Frame Error Rate*. Proportion de trames mal transmises. Voir aussi BER.

FH Faisceau hertzien. Connexion de point à point grâce aux ondes radio.

FHSS *Frequency Hopping Spread Spectrum*. Modulation radio qui consiste à sauter régulièrement d'un canal d'émission à un autre. Cette technique permet de mieux résister aux interférences localisées dans le spectre. Elle a été plus ou moins abandonnée par le WiFi, mais est à la base du Bluetooth et du HomeRF.

Firmware Microprogramme installé dans un matériel (AP, adaptateur WiFi...).

FM *Frequency Modulation*. Technique radio consistant à « moduler » la fréquence du signal émis (la « porteuse ») en fonction du signal « source ».

Fragmentation Lorsqu'un paquet à émettre parvient à la couche réseau WiFi, il peut être découpé en plusieurs fragments si sa taille dépasse un seuil fixé. Chaque fragment est ensuite envoyé indépendamment, avec ses propres en-têtes WiFi. Le paquet avant la fragmentation s'appelle le MSDU. Les fragments dotés de leur en-tête MAC s'appellent les MPDU.

FSK *Frequency Shift Keying*. Modulation radio numérique reposant sur la FM.

Full-Duplex Communication entre deux stations, chacune pouvant simultanément émettre et recevoir (voir aussi Half-Duplex).

G

GFSK *Gaussian FSK*. Le signal source numérique est d'abord passé dans un filtre Gaussien : les transitions d'état sont « adoucies ». Le résultat est modulé en FSK.

GMK *Group Master Key*. En 802.11i, clé maîtresse dont est dérivée la clé GTK.

GPRS *General Packet Radio Service*. L'une des premières technologies de 2,5G.

GSM *Global System for Mobile Communication*. Technologie de 2G.

GTK *Group Transient Key*. En 802.11i, clé dérivée de la clé GMK et servant au cryptage et contrôle d'intégrité du trafic broadcast et multicast. Voir aussi PTK.

H

Hachage Une fonction de hachage (ex. MD5) produit un nombre imprévisible à partir d'un message. Deux messages identiques donneront le même « hash », tandis que deux messages différents, même très proches, donneront deux hash sans lien entre eux.

Half-Duplex Communication entre deux stations, chacune ne pouvant pas simultanément émettre et recevoir. Voir aussi Full-Duplex.

Hand-over On parle de *hand-over* (passer la main), en mode Infrastructure, lorsqu'une station passe d'un AP à un autre, de façon transparente pour l'utilisateur.

HCCA *Hybrid Coordination Function Controlled Channel Access*. Voir EPCF.

HCF *Hybrid Coordination Function*. Autre nom de l'EPCF.

Hotspot Zone d'accès à l'Internet par le WiFi, payant ou non. Voir aussi WISP.

HR-DSSS *High Rate DSSS*. Version améliorée du DSSS introduite avec le 802.11b, permettant d'atteindre des débits plus élevés que le 802.11 DSSS grâce au CCK.

I

IAPP *Inter Access Point Protocol*. Protocole de communication entre AP (802.11F).

IBSS *Independent BSS*. Réseau composé de plusieurs stations en mode Ad Hoc.

ICI *Inter Channel* (ou *Carrier*) *Interference*. Interférence entre signaux situés sur des fréquences proches.

ICNIRP *International Commission on Non-Ionizing Radiation Protection*. Commission internationale de protection contre les ondes radio non-ionisantes.

ICV *Integrity Check Value*. Code d'intégrité du WEP.

IEEE *Institute of Electrical and Electronics Engineers*. Organisme de standardisation américain, notamment à l'origine du 802.11, sur lequel le WiFi repose.

IETF *Internet Engineering Task Force*. Organisme informel à l'origine des principaux standards de l'Internet.

IGC Infrastructure à gestion de clé. Une IGC est une organisation et des moyens techniques permettant la création, la distribution et la maintenance de clés cryptographiques, utiles pour divers services de sécurité. Voir aussi PKI.

Infrastructure Dans un réseau WiFi de type Infrastructure, chaque station est associée à un AP et ne communique que par son intermédiaire. Voir aussi Ad Hoc.

IrDA *Infrared Data Association*.

ISI *Inter Symbole Interference*. Dans des conditions de multipath, deux symboles successifs peuvent atteindre simultanément le récepteur et provoquer des inter-férences.

ISO *International Organization for Standardization*.

ITU *International Telecommunication Union*.

L

LAN *Local Area Network*. Réseau de dimension « locale » : réseau d'entreprise, réseau familial, etc. Voir aussi PAN, MAN, WAN.

LDAP *Lightweight Directory Access Protocol*. Protocole d'accès à un annuaire.

LEAP *Lightweight EAP*. Protocole de sécurité WiFi, précurseur du WPA, défini par Cisco : repose sur le 802.1x et la rotation automatique de clés WEP.

LLC *Logical Link Control*. Couche réseau définie par l'IEEE (802.2), au-dessus de la couche MAC. Elle sert d'interface unique entre les couches 2 et 3 du modèle OSI.

LoS *Line of Sight*. En condition LoS, aucun obstacle n'affecte le signal. Voir aussi NLoS.

LS Ligne spécialisée. Une LS est une liaison filaire (en général en fibre optique) reliant deux points, à très haut débit.

M

MAC *Media Access Control*. Couche réseau définie par l'IEEE en bas de la deuxième couche du modèle OSI. Elle gère notamment le partage du média entre plusieurs stations et varie selon la technologie utilisée (WiFi, Ethernet...).

MAC *Message Authentication Code*. Voir aussi MIC.

MAN *Metropolitan Area Network*. Réseau de l'échelle d'un campus ou d'une ville. Il est généralement composé de multiples LAN reliés entre eux. Voir aussi PAN, LAN, WAN.

MD5 *Message Digest 5*. Algorithme de hachage très utilisé. Voir aussi Hachage.

MIC *Message Integrity Code*. Nombre calculé à partir d'un message et envoyé avec celui-ci. Le récepteur peut ainsi s'assurer que le message n'a pas été modifié.

Michael Algorithme de contrôle d'intégrité utilisé par TKIP. Voir aussi MIC.

MiM *Man in the Middle* (également noté MitM). Une attaque MiM consiste pour un pirate à s'interposer entre deux stations du réseau, à leur insu, de façon à espionner leurs échanges, voire à les modifier.

MIMO *Multiple Input Multiple Output*. Technique radio consistant à utiliser plusieurs antennes en émission et en réception simultanément sur un même canal. Ceci permet d'atteindre une portée et un débit plus grands, en exploitant les parcours multiples du signal (multipath). Voir 802.11n.

MPDU *MAC Protocol Data Unit*. Voir Fragmentation.

MSDU *MAC Service Data Unit*. Voir Fragmentation.

MTU *Maximum Transfer Unit*. Taille maximale des paquets sur un réseau.

Multicast Trafic réseau adressé à un groupe de stations. Voir aussi Broadcast et Unicast.

Multipath On parle de multipath lorsque le signal peut parcourir plusieurs chemins entre l'émetteur et le récepteur, du fait de réflexions et diffractions sur des obstacles.

N

NAS *Network Access Server*. Contrôleur d'accès au réseau dans l'architecture RADIUS : lorsqu'un utilisateur cherche à se connecter au réseau via le NAS, celui-ci interroge le serveur RADIUS pour savoir s'il doit laisser passer l'utilisateur, ou non.

NLoS *Near Line of Sight*. Opposé du LoS.

O

OFDM *Orthogonal Frequency Division Multiplexing*. Modulation radio utilisée notamment par le 802.11a et le 802.11g. Elle consiste à diviser un canal radio en de multiples canaux et à utiliser tous ces canaux simultanément.

OIT Organisation internationale du travail.

OMS Organisation mondiale de la santé.

OSI *Open Systems Interconnection*. Conçu par l'ISO, le modèle OSI définit comment les protocoles réseaux doivent être organisés en couches superposées. Bien qu'il ne soit pas utilisé tel quel, le modèle OSI reste un modèle de référence.

P

PAC *Protected Access Credentials*. Clé cryptographique stockée dans un fichier protégé par un mot de passe. L'EAP/FAST de Cisco utilise notamment des PAC.

PAN *Personal Area Network*. Réseau de très petite taille, centré autour d'une personne. Par exemple, un PDA et un ordinateur interconnectés forment un PAN.

PBCC *Packet Binary Convolutionnary Code*. Modulation radio utilisée par le 802.11b+ et optionnelle dans le 802.11g.

PCF *Point Coordination Function*. Stratégie de partage des ondes définie par le 802.11 (optionnelle). Deux phases alternent sans cesse : dans la première, l'AP donne la parole successivement à chaque station. Dans la seconde, le mode DCF est utilisé. Le PCF permet de gérer quelques aspects de la QoS, mais le 802.11e va bien plus loin.

PEAP *Protected EAP*. Méthode d'authentification EAP établissant un tunnel TLS au sein duquel une autre authentification EAP est réalisée et ainsi protégée. Voir aussi TTLS.

PIRE Puissance isotrope rayonnée équivalente. Le PIRE d'un système radio est égal à la puissance de l'émetteur, moins les pertes dans les câbles et les connecteurs, plus le gain de l'antenne.

PKI *Public Key Infrastructure*. Voir aussi IGC.

PLCP *Physical Layer Convergence Procedure*. Couche réseau définie par l'IEEE en haut de la couche physique.

PM *Phase Modulation*. Technique radio consistant à « moduler » la phase du signal émis (la « porteuse ») en fonction du signal « source ».

PMK *Pairwise Master Key*. En 802.11i, clé maîtresse dont est dérivée la clé PTK.

PoE *Power over Ethernet*. Technologie permettant d'utiliser un câble réseau pour l'alimentation électrique d'un équipement. Voir aussi 802.3af.

POS *Personal Operating Space*. Espace occupé par un PAN.

PSK *Phase Shift Keying*. Modulation radio numérique reposant sur la PM.

PSK *Pre Shared Key*. Voir WPA-Personal.

PSM *Power Save Polling Mode* (ou PSPM). Mode d'économie d'énergie (voir aussi CAM).

PTK *Pairwise Transient Key*. En 802.11i, clé dérivée de la clé PMK et servant au cryptage et contrôle d'intégrité du trafic unicast.

Q

QAM *Quadrature Amplitude Modulation*. Modulation numérique reposant à la fois sur les modulations AM et PM.

QoS *Quality of Service*. Pour gérer la qualité de service en WiFi (par exemple, pour donner une priorité plus importante au trafic multimédia), il est nécessaire d'utiliser le PCF, ou le 802.11e (l'EDCF ou l'EPCF).

QPSK *Quadrature PSK* (également noté 4PSK). PSK avec des symboles de 2 bits.

R

RADIUS *Remote Authentication Dial In User Service*. Protocole de type AAA. Un réseau d'entreprise sécurisé par le WPA repose généralement sur un serveur RADIUS.

RC4 *Rivest Cipher 4* (ou *Ron's Code 4*). Algorithme de cryptage par flux : il produit un flux de bits pseudo aléatoires, à partir d'une clé. Ces bits sont combinés aux bits d'un message, avec l'opération XOR. Le WEP et le TKIP reposent sur RC4.

RLAN *Radio LAN*. Réseau local reposant sur une technologie radio (ex. WiFi).

Roaming Un accord de roaming entre deux opérateurs permet aux clients de l'un d'utiliser le réseau de l'autre. Par exemple, l'accord de roaming entre Wifirst et Tiscali permet aux clients de Tiscali de se connecter aux hotspots de Wifirst. Certains utilisent également le mot « roaming » pour parler de hand-over.

RSB Rapport signal/bruit (également noté S/B). Différence entre la puissance du signal (exprimé en dBm) et la puissance du bruit (également en dBm).

RSN *Robust Security Network*. Réseau WiFi sécurisé par le 802.11i. Voir TSN.

RTS/CTS *Request to Send/Clear to Send*. Lorsqu'un paquet de données doit être envoyé, si sa taille dépasse un seuil donné (le RTS Threshold), une requête RTS est d'abord envoyée pour demander la permission. Si le récepteur autorise l'envoi du paquet, il renvoie une réponse CTS à l'émetteur. Ce mécanisme permet de réduire les collisions dues aux stations qui ne sont pas à portée les unes des autres et ne peuvent donc pas savoir si elles risquent de prendre la parole en même temps.

S

Sniffer Enregistrer les paquets échangés entre des stations WiFi dans le but de superviser (ou de pirater) le réseau.

SNR *Signal to Noise Ratio* (également noté S/N). Voir RSB.

SSID *Service Set Identifier*. Voir ESSID.

SSL *Secure Socket Layer*. Voir TLS.

Station Tout équipement capable de se connecter à un réseau (ordinateur, PDA...).

STP *Spanning Tree Protocol*. Protocole défini dans la norme 802.1D et mis en œuvre dans des commutateurs (switchs) afin de mettre en œuvre une topologie maillée.

Symbole Certaines modulations radio permettent de coder plusieurs bits d'information dans un seul signal radio. On parle alors de « symbole ». Par exemple, en FSK, si huit fréquences sont définies (on parle de 8FSK), alors un signal émis sur l'une de ces fréquences porte trois bits d'information (car 23 = 8).

T

TC *Traffic Class*. Le trafic réseau peut être associé à différentes classes, en fonction de sa nature (e-mail, navigation web...), de sa provenance, sa destination, ou de tout autre paramètre. Ces classes de trafic peuvent être traitées différemment selon la politique de QoS mise en place. Voir 802.11e.

TIM *Traffic Indication Map*. Dans chaque balise, un AP peut indiquer la liste des stations en mode d'économie d'énergie pour lesquelles il possède des paquets en attente. Ces stations peuvent choisir quand demander à recevoir ces paquets.

TKIP *Temporal Key Integrity Protocol*. Protocole de sécurité WiFi reposant sur RC4 et conçu pour résoudre tous les problèmes du WEP sans avoir à changer de matériel. Le WPA repose sur TKIP. Le WPA2 repose sur TKIP ou CCMP.

TLS *Transport Layer Security*. Protocole permettant de mettre en place un tunnel sécurisé entre un client et un serveur. TLS est standardisé par l'IETF et issu du protocole SSL conçu par Netscape.

TPC *Transmit Power Control*. Adaptation automatique de la puissance de l'émetteur en fonction des conditions de transmission.

TSN *Transitional Security Network*. Réseau WiFi mixte, acceptant les stations sécurisées par le 802.11i ou le WEP. Il s'agit d'une étape de transition vers le RSN.

TTLS *Tunneled TLS*. Méthode d'authentification EAP très similaire à PEAP.

TXOP *Transmit Opportunity*. En 802.11e, lorsqu'une station obtient la parole, elle peut la conserver pendant une durée précise et émettre plusieurs paquets d'affilée.

U

Unicast Trafic réseau adressé à une seule station. Voir Broadcast et Multicast.

UWB *Ultra Wideband*. Modulation radio consistant à émettre sur une très large bande de fréquences. À courte distance, il est possible d'atteindre des débits très élevés.

V

VFIR *Very Fast Infrared*. Technologie WLAN sur infrarouges, définie par l'IrDA.

VLAN *Virtual LAN*. Plusieurs réseaux virtuels peuvent être mis en œuvre sur une même infrastructure matérielle : chaque paquet contient alors un nombre (le VLAN ID) indiquant le VLAN auquel il appartient. Les VLAN sont mis en œuvre par des commutateurs et des AP compatibles avec la norme 802.1Q.

VoIP *Voice over IP*. Technologies permettant la transmission de la voix sur un réseau IP comme Internet. Les plus utilisées sont H.323 et SIP.

VoWIP *Voice over Wireless IP*. VoIP par le biais d'un réseau sans fil.

W

WAN *Wide Area Network*. Réseau de dimension nationale ou mondiale, par exemple l'Internet. Voir aussi PAN, LAN, WAN.

WarDriving Promenade en voiture pour détecter des réseaux WiFi.

WDS *Wireless Distribution System*. Connexion sans fil entre AP. Voir aussi DS.

WECA *Wireless Ethernet Compatibility Alliance*. Voir WiFi Alliance.

WEP *Wired Equivalent Privacy*. Première solution de sécurité du 802.11, reposant sur le RC4. Ses défauts sont nombreux et il vaut mieux passer au WPA ou WPA2.

WiFi Certification de la WiFi Alliance pour les produits respectant la norme 802.11.

WiFi Alliance Association de constructeurs de produits WiFi.

WiMAX Technologie de WMAN définie par le WiMAX Forum à partir des normes IEEE 802.16 et ETSI HiperMAN.

WISP *Wireless ISP*. FAI dont les clients peuvent se connecter à des hotspots.

WLAN *Wireless LAN*. Réseau local sans fil (WiFi, VFIR...). Voir RLAN.

W-Link Association française dont le but est de promouvoir le roaming entre WISP.

WMAN *Wireless MAN*. Réseau MAN sans fil (WiMAX, BLR...).

WME *Wireless Multimedia Extensions*. Voir WMM.

WMM *WiFi MultiMedia*. Certification de la WiFi Alliance pour les produits WiFi compatibles avec le mode EDCF de la norme 802.11e.

WMM-Scheduled Access Certification de la WiFi Alliance pour les produits WiFi compatibles avec le mode EPCF de la norme 802.11e.

WPA *Wireless Protected Access*. Certification de la WiFi Alliance pour les produits WiFi compatibles avec la sécurité TKIP définie par la norme 802.11i.

WPA-Personal Certification pour les produits WPA que l'on peut configurer avec une clé secrète (PSK), partagée par tous les équipements du réseau, sans serveur d'authentification. On parle également de WPA/PSK.

WPA-Enterprise Certification pour les produits WPA compatibles avec la norme 802.1x. L'architecture 802.1x implique la mise en place d'un serveur d'authentification (généralement de type RADIUS).

WPA2 Certification de la WiFi Alliance pour les produits WiFi gérant la sécurité 802.11i complète et notamment le CCMP/AES.

WPAN *Wireless PAN*. Réseau PAN sans fil (Bluetooth, ZigBee...).

WWAN *Wireless WAN*. Réseau WAN sans fil (2,5G, 3G, 802.20...).

X-Z

XOR *Exclusive Or*. Le « ou exclusif » est une addition binaire sans retenue (1 + 1 = 0).

ZigBee Technologie de WPAN à faible consommation électrique mais bas débit.

Webographie

Retrouvez ces références, ainsi que les annexes, des commentaires, des informations et d'éventuelles corrections sur le site web du livre : *www.livrewifi.com*.

Portails et tutoriels

WiFi Planet – http://www.wi-fiplanet.com/

WiFi Networking News – http://wifinetnews.com/

Comment ça marche ? – http://www.commentcamarche.net/wifi/

Wireless DevCenter – http://www.oreillynet.com/wireless/

Wikipedia – http://fr.wikipedia.org/wiki/802.11

Adminet – http://www.admi.net/cgi-bin/wiki?WiFi

Féd. Internet Nouv. Gén. – http://www.fing.org/

Produits

WiFi Alliance – http://www.wi-fi.org/

WiFi Planet – http://products.wi-fiplanet.com/

FWT – http://www.fwt.fr/

Equip. Scient. – http://www.es-france.com/

Surcouf – http://www.surcouf.com/

Organismes

ANF – http://www.anfr.fr/

ARCEP – http://www.arcep.fr/

CNIL – http://www.cnil.fr/

DiGITIP – http://www.telecom.gouv.fr/

ETSI – http://www.etsi.org/

IEEE – http://www.ieee.org/

IETF – http://www.ietf.org/

ISO – http://www.iso.org/

W-link – http://www.w-link.fr/

WiFi Alliance – http://www.wi-fi.org/

Associations

France Wireless – http://www.wireless-fr.org/

FreeNetworks.org – http://www.freenetworks.org/

Nantes Wireless – http://www.nantes-wireless.org/

Personal Telco – http://www.personaltelco.net/

WISP

Boingo – http://www.boingo.com/

Bouygues Télécom – http://www.bouyguestelecom.fr/

iPass – http://www.ipass.com/

Orange – http://www.orange-wifi.com/

SFR – http://wifi.sfr.fr/

Wifirst – http://www.wifirst.net/

Logiciels

AirMagnet – http://www.airmagnet.com/ – Analyse & supervision WiFi

Air Traf – http://www.elixar.com/ – Analyse & supervision WiFi

AP Grapher – http://www.chimoosoft.com/ – Analyseur WiFi simple

AP Radar – http://apradar.sourceforge.net/ – Client WiFi pour Linux

AirSnort – http://airsnort.shmoo.com/ – Outil de hacking WEP

Ethereal – http://www.ethereal.com/ – Analyseur de réseau

EtherPeek – http://www.wildpackets.com/ – Analyseur de réseau

FreeRADIUS – http://www.freeradius.org/ – Serveur RADIUS libre

Kismet – http://www.kismetwireless.net/ – Outil de hacking WiFi

NetStumbler – http://www.stumbler.net/ – Analyseur WiFi

Odyssey – http://www.juniper.net/ – Client et serveur RADIUS

Open1x – http://open1x.sourceforge.net/ – Client 802.1x Open Source

Packetyzer – http://www.packetyzer.com/ – Analyseur réseau

Skype – http://www.skype.com/ – Logiciel de voix sur IP (VoIP)

TCPDump – http://www.tcpdump.org/ – Outil d'analyse réseau

Weplab – http://weplab.sourceforge.net/ – Outil de hacking WEP

Standard 802.11 – http://ieee802.org/11/

RFC – http://www.ietf.org/rfc[1]

RFC 768 – *User Datagram Protocol* (UDP)

RFC 791 – *Internet Protocol* (IP)

RFC 793 – *Transmission Control Protocol* (TCP)

RFC 1321 – Algorithme Message-Digest 5 (MD5)

RFC 1334 – Protocoles d'authentification pour PPP

RFC 1661 – *Point-to-Point Protocol* (PPP)

RFC 1994 – *Challenge Handshake Authentication Protocol* (CHAP)

RFC 2104 – *Keyed-Hashing for Message Authentication* (HMAC)

RFC 2246 – Protocole TLS version 1.0

RFC 2289 – Système *One-Time Password* (OTP)

RFC 2433 – Extensions Microsoft de CHAP (MS-CHAP-v1)

RFC 2548 – Attributs RADIUS *Vendor-specific* de Microsoft

RFC 2716 – Authentification EAP/TLS

RFC 2759 – Extensions Microsoft de CHAP, version 2 (MS-CHAP-v2)

RFC 2809 – *Implementation de L2TP Compulsory Tunneling via* RADIUS

1. Pour les RFC en français, consultez le site *http://abcdrfc.free.fr/*

RFC 2865 – *Remote Authentication Dial In User Service* (RADIUS)

RFC 2866 – RADIUS *Accounting*

RFC 2867 – Modifications du RADIUS *Accounting* pour le support des tunnels

RFC 2868 – Attributs RADIUS pour le support des tunnels

RFC 2869 – RADIUS *Extensions*

RFC 3078 – Protocole *Microsoft Point-To-Point Encryption* (MPPE)

RFC 3579 – EAP sur RADIUS

RFC 3588 – Protocole Diameter

RFC 3748 – *Extensible Authentication Protocol* (EAP)

RFC 4186 – EAP-SIM

RFC 4187 – EAP-AKA

Drafts[1] – http://www.ietf.org/internet-drafts/

EAP/MS-CHAP-v2 – draft-ietf-pppext-mschap-v2

EAP/PEAP – draft-josefsson-pppext-eap-tls-eap

EAP/TTLS – draft-funk-eap-ttls

Portails de technologies alternatives

BLR – http://blr.free.fr/

Bluetooth – http://www.bluetooth.com/

CPL – http://www.cpl-france.org/

DECT – http://www.dectweb.com/

Ethernet – http://ieee802.org/3/

HomePlug – http://www.homeplug.org/

HomeRF – http://www.palowireless.com/homerf/

Infrarouge – http://www.irda.org/

PoE – http://www.poweroverethernet.com/

UMTS – http://www.umts-forum.org/

WiMAX – http://www.wimaxforum.org/

ZigBee – http://www.zigbee.org/

1. Certains *drafts* sont susceptibles de disparaître ou d'être promus au rang de RFC.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

INFOPRO

TYPE D'OUVRAGE

L'ESSENTIEL	SE FORMER	RETOURS D'EXPÉRIENCE

MANAGEMENT DES SYSTÈMES D'INFORMATION
APPLICATIONS MÉTIERS
ÉTUDES, DÉVELOPPEMENT, INTÉGRATION
EXPLOITATION ET ADMINISTRATION
RÉSEAUX & TÉLÉCOMS

Aurélien Géron
Préface de Marc Taieb

WIFI PROFESSIONNEL

La norme 802.11, le déploiement, la sécurité

3e édition

L'objectif de ce livre est de vous aider à bâtir un réseau sans fil professionnel et sécurisé :

– La première partie vous permettra de comprendre le WiFi et les rouages de la **norme 802.11** : des modulations radio (DSSS, OFDM, MIMO…) à la gestion de la **QoS** (802.11e, WMM). Elle dresse un panorama des technologies alternatives, du futur du WiFi et des perspectives ouvertes par la **voix sur IP sans fil**.

– La deuxième partie vous permettra de **concevoir et déployer un réseau WiFi** de qualité professionnelle. Vous saurez choisir le matériel adéquat, réaliser une cartographie radio, gérer les obstacles et les interférences, et superviser votre réseau.

– La troisième partie vous donnera toutes les armes pour sécuriser au mieux votre réseau sans fil. Vous connaîtrez les attaques possibles, les **bonnes pratiques** et les technologies pour vous protéger : WEP, VPN, 802.1x, WPA et **WPA2**. Vous découvrirez également les serveurs d'authentification **RADIUS** qui sont au cœur des réseaux WiFi d'entreprise.

Cette troisième édition comporte un grand nombre de mises à jour notamment sur **la réglementation et la santé**, les évolutions des normes (802.11e, 802.11n, 802.11s…), les commutateurs intelligents qui gagnent du terrain, et les technologies connexes qui ont évolué.

Suppléments gratuits en ligne sur le site
www.livrewifi.com

AURÉLIEN GÉRON
est cofondateur et directeur technique de la société Wifirst, premier fournisseur d'accès à Internet sans fil en France. Il est co-auteur de deux ouvrages parus chez Dunod sur les architectures Internet et sur la programmation C++ avancée.

ISBN 978-2-10-054183-6

DUNOD
www.dunod.com