

Avant-propos

La technologie Wi-Fi 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 des Télécommunications (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. Effectivement, les concurrents sérieux se bousculent : HiperLAN, Bluetooth, WiMAX, voire GPRS ou UMTS.

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 Wi-Fi a réellement conquis le grand public. Les grands opérateurs proposent dorénavant des abonnements ADSL avec des modems Wi-Fi 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 Wi-Fi. 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 Wi-Fi.

Le Wi-Fi 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 Wi-Fi 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, et ainsi de suite. Toutefois, concevoir et maintenir un réseau Wi-Fi d'entreprise, sécurisé, rapide, disponible dans tous les bureaux et bien administré, est une autre gageure que de connecter quelques ordinateurs à un réseau Wi-Fi 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 Wi-Fi de façon aussi exhaustive que possible, pour les entreprises désireuses de passer au Wi-Fi, 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 démuné lorsqu'on lui demande de « wifiser » son entreprise et qu'il cherche la littérature adaptée. 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 aucun n'offre 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 Wi-Fi : chapitres 1 à 3 ;
- déployer votre réseau sans fil : chapitres 4 et 5 ;
- sécuriser votre réseau sans fil : chapitres 6 à 10.

Première partie : comprendre le Wi-Fi

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

Le chapitre 1 présente une vue d'ensemble du Wi-Fi, son contexte historique, technique et commercial et ses principales applications. Les technologies alternatives sont également abordées : l'HiperLAN, le HomeRF, le Bluetooth, le WiMAX, etc.

Les chapitres 2 et 3 détaillent la norme 802.11 sur laquelle repose le Wi-Fi. Le chapitre 2 se concentre sur les couches physiques et présente les variantes du Wi-Fi : le 802.11a, 802.11b et 802.11g. Le chapitre 3 présente la couche MAC du protocole 802.11, c'est-à-dire le « cerveau » du Wi-Fi, qui offre de nombreuses fonctionnalités essentielles.

Seconde 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 Wi-Fi, des adaptateurs Wi-Fi aux points d'accès (les AP, c'est-à-dire les bornes Wi-Fi) en passant par les antennes et les téléphones Wi-Fi. 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 de sécurité du Wi-Fi : vous saurez comment mettre en place un réseau sans fil tout aussi sûr que votre réseau filaire grâce à la norme 802.11i et au WPA.

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, et elle est malheureusement complètement insuffisante. Toutefois, elle est encore très répandue et doit donc être présentée. Ses failles sont expliquées en détail.

Le chapitre 8 présente le protocole 802.1x dont le rôle est d'identifier les utilisateurs et de préparer une connexion sécurisée au réseau. Ce protocole simple et générique est à la base de nombreuses solutions de sécurité dont le 802.11i et le WPA.

Le chapitre 9 présente le 802.11i et le WPA, les deux solutions « miracles » du Wi-Fi, qui offrent un niveau de sécurité jusqu'ici inégalé. Nous vous conseillons fortement de mettre en place une sécurité WPA ou 802.11i sur votre réseau Wi-Fi.

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 802.11i et le WPA.

Les annexes

Ce livre comporte trois annexes qui présentent des sujets divers, utiles pour comprendre certaines parties de cet ouvrage, mais trop éloignés du Wi-Fi 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 vous sera sans doute utile assez fréquemment. Toutefois, chaque sigle est 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 toutefois recommandé de lire le chapitre 1 qui offre une vision globale du Wi-Fi et le chapitre 6 qui présente la sécurité dans ses grandes lignes. Les chapitres 2 et 3 présentent la norme 802.11 en détail, et 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 Wi-Fi robuste et sécurisé, et une référence 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, Alexis PASTRÉ, Aurélien RICARD, Gaël GAUDIN 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 guidé dans les dédales obscurs de la langue française.

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 Wi-Fi.