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

Toutes les marques citées dans cet ouvrage sont des marques déposées par leurs propriétaires respectifs.

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

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.
Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.
Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).



© Dunod, Paris, 2004, 2006, 2009

ISBN 978-2-10-054183-6

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2° et 3° a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).
Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

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

Préface III

Avant-propos XV

Première partie – Comprendre le WiFi

Chapitre 1 – Contexte et applications du WiFi 3

1.1 Un boom à retardement 3

1.1.1 De l'histoire ancienne 3

1.1.2 Les raisons du retard 4

1.1.3 Le boom du WiFi 6

1.2 Quelques rappels sur les réseaux 8

1.2.1 Les réseaux et les protocoles 8

1.2.2 Les couches de protocoles 8

1.2.3 Le modèle OSI 10

1.2.4 La typologie des réseaux 11

1.2.5 Les WLAN 12

1.2.6 Les standards de l'IEEE 14

1.3 Les applications du WiFi 15

1.3.1 L'extension du réseau d'entreprise 15

1.3.2 Le WiFi à domicile 15

1.3.3 Les hotspots 16

1.3.4 Le WiFi communautaire 19
1.3.5 Le point à point 21
1.3.6 Le WiFi dans l'industrie 21
1.4 Les technologies alternatives 23
1.4.1 L'Ethernet 23
1.4.2 Le CPL 23
1.4.3 L'infrarouge et le laser 24
1.4.4 Le Bluetooth 25
1.4.5 La « data mobile » 25
1.4.6 Autres technologies 26
1.4.7 La place du WiFi 27

Chapitre 2 – La norme 802.11 : couches physiques 29
2.1 Une vue d'ensemble 29
2.1.1 Trois couches physiques 30
2.1.2 Une couche MAC 30
2.1.3 Les évolutions du 802.11 30
2.2 Quelques rappels sur les ondes radio 31
2.2.1 Les grandeurs physiques des ondes 31
2.2.2 Les règles de la transmission radio 33
2.3 Les modulations radio 38
2.3.1 Les modulations fondamentales 38
2.3.2 Les modulations numériques 40
2.3.3 Le FHSS 44
2.3.4 Le DSSS 45
2.3.5 L'OFDM 47
2.3.6 Techniques multi-antennes 49
2.4 Les canaux 55
2.4.1 Les canaux à 2,4 GHz 55
2.4.2 Les canaux à 5 GHz 57
2.4.3 Regroupement de canaux 58
2.5 Les trames 802.11 59
2.5.1 La structure d'une trame 59
2.5.2 Le préambule 59

2.5.3 L'en-tête PLCP 60
2.6 La norme 802.11n 61
2.6.1 La norme 802.11n et ses « drafts » 61
2.6.2 Un meilleur débit et une plus grande portée 61
2.6.3 Les principales améliorations du 802.11n 62

Chapitre 3 – La norme 802.11 : couche MAC 65
3.1 Tour d'horizon de la couche MAC 65
3.1.1 Les couches LLC et MAC 65
3.1.2 Les fonctions de la couche MAC 66
3.1.3 Les évolutions de la couche MAC 67
3.1.4 Un rappel sur l'Ethernet 69
3.2 Le partage des ondes en WiFi 73
3.2.1 Le mode DCF 73
3.2.2 Le mode PCF 75
3.2.3 Les améliorations du 802.11e 77
3.2.4 Le paramétrage et la compatibilité 80
3.3 Le réseau Ad Hoc ou Infrastructure 81
3.3.1 Le mode Infrastructure 82
3.3.2 Le mode Ad Hoc et les réseaux maillés 82
3.4 Le processus d'association 85
3.4.1 Les trames « balises » 85
3.4.2 Détecter les réseaux présents 85
3.4.3 L'authentification 86
3.4.4 L'association 88
3.4.5 La réassociation 88
3.4.6 Et en mode Ad Hoc ? 89
3.5 Les mécanismes de sécurité 89
3.5.1 Masquer le SSID 89
3.5.2 Filtrage par adresse MAC 90
3.5.3 Le WEP 90
3.5.4 Le 802.11i et le WPA 91
3.6 Les autres fonctions MAC 92
3.6.1 Le contrôle d'erreur 92

3.6.2 La fragmentation ... 92
3.6.3 L'acheminement des paquets et le WDS ... 93
3.6.4 L'économie d'énergie ... 95
3.6.5 Le WMM-PS ... 98
3.7 Les paquets WiFi ... 99
3.7.1 La structure des paquets ... 99
3.7.2 Les types de paquets ... 101
3.7.3 Les couches supérieures ... 103
3.8 Les améliorations du 802.11n ... 104
3.8.1 L'agrégation de trames ... 104
3.8.2 Acquittements groupés ... 105

Deuxième partie – Déploiement

Chapitre 4 – Le matériel ... 109
4.1 Les adaptateurs ... 109
4.1.1 Le rôle de l'adaptateur ... 109
4.1.2 La connectique ... 110
4.1.3 Le pilote ... 112
4.2 Le point d'accès ... 114
4.2.1 Le pont vers un réseau filaire ... 114
4.2.2 Le point d'accès répétiteur ... 117
4.2.3 Les réseaux multiples ... 121
4.2.4 Le routeur ... 125
4.2.5 Le hotspot et le contrôleur d'accès ... 126
4.2.6 La configuration d'un AP ... 132
4.2.7 Comment choisir un AP ? ... 132
4.3 Les périphériques WiFi ... 135
4.3.1 Les périphériques de bureautique ... 135
4.3.2 Les outils d'analyse ... 137
4.3.3 Les périphériques « industriels » ... 139
4.3.4 La téléphonie sur WiFi ... 140
4.4 Les antennes WiFi ... 141
4.4.1 Comprendre les antennes ... 141

4.4.2 Les formats d'antennes ... 145
4.4.3 Les câbles et les connecteurs d'antennes ... 147
4.5 Le matériel pour le déploiement ... 147
4.5.1 Le PoE ... 147
4.5.2 Le CPL ... 149
4.5.3 Les filtres passe-bande et les atténuateurs ... 149

Chapitre 5 – La couverture radio ... 153
5.1 Le bilan radio ... 153
5.1.1 Un schéma général ... 153
5.1.2 Un exemple de point à point ... 156
5.1.3 Comment améliorer le bilan radio ? ... 157
5.2 Les perturbations radio ... 161
5.2.1 Le bruit et les interférences ... 161
5.2.2 L'absorption et la réflexion ... 163
5.2.3 La polarisation ... 165
5.2.4 La diffraction ... 166
5.2.5 Les chemins multiples (multipath) ... 168
5.2.6 Les zones de Fresnel ... 171
5.2.7 La disponibilité d'une liaison point à point ... 174
5.3 Déployer de multiples AP ... 175
5.3.1 La densité d'AP et le débit ... 175
5.3.2 Limiter les interférences entre AP ... 176
5.3.3 Les réseaux sans fil à haute capacité ... 179
5.3.4 L'audit de site ... 183
5.3.5 L'installation des AP ... 190

Troisième partie – Sécurité

Chapitre 6 – La sécurité sans fil ... 195
6.1 Introduction à la sécurité ... 195
6.1.1 Définir la sécurité ... 195
6.1.2 Une politique globale ... 197
6.1.3 La compartimentation ... 198

6.1.4 *La connexion à Internet* 200
6.1.5 *L'évolution de la sécurité* 200
6.2 Les attaques d'un réseau WiFi 201
6.2.1 *Le wardriving* 201
6.2.2 *L'espionnage* 203
6.2.3 *L'intrusion* 203
6.2.4 *Le déni de service* 207
6.2.5 *La modification des messages* 209
6.3 Les premières solutions 212
6.3.1 *Limiter les débordements* 212
6.3.2 *Éviter les AP pirates* 212
6.3.3 *La supervision radio* 212
6.3.4 *Masquer le SSID* 213
6.3.5 *Le filtrage par adresse MAC* 213
6.3.6 *Les VLAN* 213
6.3.7 *Le cryptage WEP* 214
6.3.8 *Isoler le réseau sans fil* 215
6.3.9 *Les réseaux privés virtuels* 216
6.4 Les nouvelles solutions de sécurité 217
6.4.1 *La mort du WEP* 217
6.4.2 *Le LEAP et les solutions propriétaires* 218
6.4.3 *Le WPA* 218
6.4.4 *Le 802.11i (WPA2)* 218

Chapitre 7 – Le WEP 221
7.1 La mise en œuvre 221
7.1.1 *Déployer le WEP* 221
7.1.2 *La rotation des clés* 223
7.1.3 *Les clés individuelles* 224
7.2 Les rouages du WEP 227
7.2.1 *L'algorithme RC4* 227
7.2.2 *Crypter avec RC4* 227
7.2.3 *Éviter la répétition de la clé RC4* 229
7.2.4 *Le vecteur d'initialisation* 230

7.2.5 L'authentification WEP 231
7.2.6 Le contrôle d'intégrité 231
7.3 Les failles 233
7.3.1 Les failles du cryptage 233
7.3.2 Les failles de l'authentification 237
7.3.3 Les failles du contrôle d'intégrité 238

Chapitre 8 – Le 802.1x 241
8.1 L'origine d'EAP 242
8.1.1 L'IETF 242
8.1.2 Le protocole PPP 242
8.1.3 L' authentification avec PPP 243
8.2 Le fonctionnement d'EAP 245
8.2.1 L'architecture : trois acteurs 245
8.2.2 Les dialogues : quatre paquets 249
8.2.3 L'EAP et le 802.1x 251
8.3 Les méthodes EAP 253
8.3.1 EAP/MD5 253
8.3.2 EAP/MS-CHAP-v2 253
8.3.3 EAP/OTP 253
8.3.4 EAP/GTC 254
8.3.5 EAP/SIM 255
8.3.6 EAP/TLS 255
8.3.7 EAP/PEAP 257
8.3.8 EAP/TTLS 259
8.3.9 PEAP ou TTLS ? 260
8.3.10 EAP/FAST 260
8.3.11 Autres méthodes EAP 262
8.4 La sécurité d'EAP 263
8.4.1 Les failles 263
8.4.2 L'attaque de la méthode EAP 263
8.4.3 L'attaque de la session 264
8.4.4 Les attaques MiM 266
8.4.5 Une bonne sécurité avec le 802.1x 269

Chapitre 9 – Le WPA et le WPA2 271

9.1 Déployer le WPA ou le WPA2 271

9.1.1 Rappels et définitions 271

9.1.2 Le WPA Personal 272

9.1.3 Le WPA Enterprise 274

9.2 La distribution des clés 276

9.2.1 Une connexion complète 276

9.2.2 La hiérarchie des clés 279

9.2.3 Dérivation de la clé temporaire PTK 281

9.2.4 La rotation de la clé de groupe 284

9.2.5 Le fonctionnement en mode Ad Hoc 284

9.3 La solution TKIP 287

9.3.1 Présentation générale 287

9.3.2 Le cryptage TKIP 288

9.3.3 Empêcher la relecture 291

9.3.4 Le contrôle d'intégrité Michael 291

9.3.5 Le mode mixte : WEP et WPA 296

9.4 La solution AES 297

9.4.1 Pourquoi AES ? 297

9.4.2 Le WPA/AES 297

9.4.3 Les modes de cryptage 299

9.4.4 Le CCMP 302

Chapitre 10 – Le RADIUS 307

10.1 Les fonctions du serveur RADIUS 307

10.1.1 L'authentification 307

10.1.2 L'autorisation 311

10.1.3 La comptabilisation 312

10.2 Le protocole RADIUS 315

10.2.1 Le RADIUS et l'UDP 315

10.2.2 Les six types de paquets 317

10.2.3 Le format des paquets RADIUS 318

10.2.4 Le 802.1x et le RADIUS 320

10.3 Questions de sécurité 322
10.3.1 Le secret RADIUS 322
10.3.2 L'authenticator 323
10.3.3 L'attribut Message-Authenticator 326
10.3.4 L'attaque hors-ligne contre le secret 326
10.3.5 Le RADIUS sur Internet 327
10.3.6 Les VLAN 331
10.3.7 L'échange de la clé PMK 331

Chapitre 11 – Les obligations légales 335

11.1 Protéger la vie privée des utilisateurs du réseau 335

11.2 Lutter contre la cybercriminalité 336

11.3 Permettre la cohabitation de services sans fil voisins 338
11.3.1 Des bandes de fréquences libres 338
11.3.2 Limites pour la bande des 2,4 GHz 338
11.3.3 Limites pour la bande des 5 GHz 339
11.3.4 Comment respecter ces limites ? 339

11.4 Garantir la sécurité sanitaire 341
11.4.1 Introduction 341
11.4.2 Les effets thermiques des ondes 342
11.4.3 Les effets non thermiques 345
11.4.4 Un débat passionné 348

Glossaire 353

Webographie 367

Index 371

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.