

# Table des matières

Préface . . . . .	V
Avant-propos . . . . .	XV
<b>Première partie – Comprendre le Wi-Fi</b>	
<b>Chapitre 1 – Contexte et applications du Wi-Fi . . . . .</b>	<b>3</b>
1.1 Un boom à retardement . . . . .	3
1.1.1 <i>De l'histoire ancienne</i> . . . . .	3
1.1.2 <i>Les raisons du retard</i> . . . . .	4
1.1.3 <i>Le boom du Wi-Fi.</i> . . . . .	6
1.2 Quelques rappels sur les réseaux . . . . .	8
1.2.1 <i>Les réseaux et les protocoles</i> . . . . .	8
1.2.2 <i>Les couches de protocoles</i> . . . . .	9
1.2.3 <i>Le modèle OSI</i> . . . . .	10
1.2.4 <i>La typologie des réseaux</i> . . . . .	11
1.2.5 <i>Les WLAN</i> . . . . .	13
1.2.6 <i>Les standards de l'IEEE.</i> . . . . .	14
1.3 Les applications du Wi-Fi . . . . .	16
1.3.1 <i>L'extension du réseau d'entreprise</i> . . . . .	16
1.3.2 <i>Le Wi-Fi à domicile</i> . . . . .	16
1.3.3 <i>Les hotspots</i> . . . . .	17
1.3.4 <i>Le Wi-Fi communautaire</i> . . . . .	23
1.3.5 <i>Le point à point</i> . . . . .	24
1.3.6 <i>Le Wi-Fi dans l'industrie</i> . . . . .	24
1.4 Les technologies alternatives . . . . .	26
1.4.1 <i>L'Ethernet.</i> . . . . .	26
1.4.2 <i>Le CPL</i> . . . . .	27

1.4.3	<i>L'infrarouge et le laser</i>	29
1.4.4	<i>Le Bluetooth</i>	30
1.4.5	<i>Le ZigBee</i>	31
1.4.6	<i>L'UWB</i>	31
1.4.7	<i>L'HiperLAN</i>	32
1.4.8	<i>Le HomeRF</i>	32
1.4.9	<i>Le Wi-Fi « amélioré »</i>	32
1.4.10	<i>Les faisceaux hertziens</i>	34
1.4.11	<i>La BLR</i>	34
1.4.12	<i>La téléphonie mobile</i>	37
1.4.12	<i>Pourquoi choisir le Wi-Fi ?</i>	39
1.5	<i>Résumé</i>	41
<b>Chapitre 2 – La norme 802.11 : couches physiques</b>		43
2.1	<i>Une vue d'ensemble</i>	43
2.2	<i>Quelques rappels sur les ondes radio</i>	45
2.2.1	<i>Les grandeurs physiques des ondes</i>	45
2.2.2	<i>Les règles de la transmission radio</i>	47
2.3	<i>Les modulations radio</i>	53
2.3.1	<i>Les modulations fondamentales</i>	53
2.3.2	<i>Les modulations numériques</i>	55
2.3.3	<i>Le FHSS</i>	60
2.3.4	<i>Le DSSS</i>	61
2.3.5	<i>L'OFDM</i>	64
2.4	<i>Les canaux</i>	66
2.5	<i>Les trames 802.11</i>	68
2.5.1	<i>La structure d'une trame</i>	68
2.5.2	<i>Le préambule</i>	69
2.5.2	<i>L'en-tête PLCP</i>	70
2.6	<i>Résumé</i>	70
<b>Chapitre 3 – La norme 802.11 : couche MAC</b>		73
3.1	<i>Tour d'horizon de la couche MAC</i>	73
3.1.1	<i>Les couches LLC et MAC</i>	73
3.1.2	<i>Les fonctions de la couche MAC</i>	74
3.1.3	<i>Les évolutions de la couche MAC</i>	75
3.1.4	<i>Un rappel sur l'Ethernet</i>	77

3.2	Le partage des ondes en Wi-Fi . . . . .	82
3.2.1	Mode DCF . . . . .	82
3.2.2	Mode PCF . . . . .	85
3.2.3	Les améliorations du 802.11e . . . . .	87
3.2.4	Paramétrage et compatibilité . . . . .	90
3.3	Réseau Ad Hoc ou Infrastructure . . . . .	91
3.3.1	Mode Infrastructure . . . . .	91
3.3.2	Mode Ad Hoc et réseaux maillés . . . . .	93
3.4	Le processus d'association . . . . .	94
3.4.1	Les trames « balises » . . . . .	94
3.4.2	Détecter les réseaux présents . . . . .	95
3.4.3	L'authentification . . . . .	96
3.4.4	L'association . . . . .	98
3.4.5	La réassociation . . . . .	98
3.4.6	Et en mode Ad Hoc ? . . . . .	98
3.5	Les mécanismes de sécurité . . . . .	99
3.5.1	Masquer le SSID . . . . .	99
3.5.2	Filtrage par adresse MAC . . . . .	99
3.5.3	Le WEP . . . . .	100
3.5.4	Le 802.1x et la rotation de clé WEP . . . . .	101
3.5.5	Le 802.11i et le WPA . . . . .	102
3.6	Les autres fonctions MAC . . . . .	103
3.6.1	Le contrôle d'erreur . . . . .	103
3.6.2	La fragmentation . . . . .	103
3.6.3	L'acheminement des paquets et le WDS . . . . .	105
3.6.4	L'économie d'énergie . . . . .	107
3.7	Les paquets Wi-Fi . . . . .	110
3.7.1	La structure des paquets . . . . .	110
3.7.2	Les types de paquets . . . . .	112
3.7.3	Les couches supérieures . . . . .	115
3.8	Résumé . . . . .	116

## Deuxième partie – Déploiement

Chapitre 4 – Le matériel . . . . .	121
4.1 Les adaptateurs . . . . .	121
4.1.1 Le rôle de l'adaptateur . . . . .	121

- 4.1.2 La connectique . . . . . 122
- 4.1.3 Le pilote . . . . . 124
- 4.2 Le point d'accès . . . . . 127
  - 4.2.1 Le pont vers un réseau filaire . . . . . 127
  - 4.2.2 Le point d'accès répéteur . . . . . 130
  - 4.2.3 Les réseaux multiples . . . . . 135
  - 4.2.4 Le routeur . . . . . 139
  - 4.2.5 Le hotspot et le contrôleur d'accès . . . . . 140
  - 4.2.6 Configuration d'un AP . . . . . 147
  - 4.2.7 Résumé : comment choisir un AP ? . . . . . 148
- 4.3 Les périphériques Wi-Fi . . . . . 150
  - 4.3.1 Les périphériques de bureautique . . . . . 151
  - 4.3.2 Les outils d'analyse . . . . . 153
  - 4.3.3 Les périphériques « industriels » . . . . . 155
  - 4.3.4 La téléphonie sur Wi-Fi . . . . . 156
- 4.4 Les antennes Wi-Fi . . . . . 157
  - 4.4.1 Comprendre les antennes . . . . . 158
  - 4.4.2 Les formats d'antennes . . . . . 162
  - 4.4.3 Les câbles et les connecteurs d'antennes . . . . . 163
- 4.5 Matériel pour le déploiement . . . . . 164
  - 4.5.1 Le PoE . . . . . 164
  - 4.5.2 Le CPL . . . . . 166
  - 4.5.3 Les filtres passe-bande et les atténuateurs . . . . . 167
- 4.6 Résumé . . . . . 167
- Chapitre 5 – La couverture radio . . . . . 169**
- 5.1 Le bilan radio . . . . . 169
  - 5.1.1 Un schéma général . . . . . 169
  - 5.1.2 Un exemple de point à point . . . . . 172
  - 5.1.3 Comment améliorer le bilan radio ? . . . . . 174
- 5.2 Les perturbations radio . . . . . 177
  - 5.2.1 Le bruit et les interférences . . . . . 177
  - 5.2.2 L'absorption et la réflexion . . . . . 180
  - 5.2.3 La polarisation . . . . . 182
  - 5.2.4 La diffraction . . . . . 183
  - 5.2.5 Les chemins multiples (multipath) . . . . . 185

5.2.6	Les zones de Fresnel . . . . .	189
5.2.7	Disponibilité d'une liaison point à point . . . . .	192
5.3	Déployer de multiples AP . . . . .	193
5.3.1	Densité d'AP et débit . . . . .	193
5.3.2	Limiter les interférences entre AP . . . . .	194
5.3.5	Les réseaux sans fil à haute capacité . . . . .	198
5.3.4	L'audit de site . . . . .	202
5.3.6	L'installation des AP . . . . .	210
5.4	Résumé . . . . .	211

### Troisième partie – Sécurité

<b>Chapitre 6 – La sécurité sans fil . . . . .</b>	<b>215</b>
6.1 Introduction à la sécurité . . . . .	215
6.1.1 Définir la sécurité . . . . .	215
6.1.2 Une politique globale . . . . .	217
6.1.3 La compartimentation . . . . .	218
6.1.4 La connexion à Internet . . . . .	220
6.1.5 L'évolution de la sécurité . . . . .	221
6.2 Les attaques d'un réseau Wi-Fi . . . . .	222
6.2.1 Le WarDriving . . . . .	222
6.2.2 L'espionnage . . . . .	224
6.2.3 L'intrusion . . . . .	224
6.2.4 Le déni de service . . . . .	228
6.2.5 La modification des messages . . . . .	230
6.3 Les premières solutions . . . . .	233
6.3.1 Limiter les débordements . . . . .	233
6.3.2 Éviter les AP pirates . . . . .	234
6.3.3 La supervision radio . . . . .	234
6.3.4 Masquer le SSID . . . . .	234
6.3.5 Le filtrage par adresse MAC . . . . .	235
6.3.6 Les VLAN . . . . .	235
6.3.7 Le cryptage WEP . . . . .	236
6.3.8 Isoler le réseau sans fil . . . . .	237
6.3.9 Les réseaux privés virtuels . . . . .	238
6.4 Les nouvelles solutions de sécurité . . . . .	240
6.4.1 La mort du WEP . . . . .	240

6.4.2	LEAP et les solutions propriétaires . . . . .	240
6.4.3	Le WPA . . . . .	241
6.4.4	Le 802.11i (WPA2) . . . . .	241
6.5	Résumé . . . . .	242
<b>Chapitre 7 – Le WEP . . . . .</b>		<b>245</b>
7.1	La mise en œuvre . . . . .	245
7.1.1	Déployer le WEP. . . . .	245
7.1.2	La rotation des clés . . . . .	247
7.1.3	Les clés individuelles . . . . .	249
7.2	Les rouages du WEP . . . . .	252
7.2.1	L'algorithme RC4 . . . . .	252
7.2.2	Crypter avec RC4 . . . . .	253
7.2.3	Éviter la répétition de la clé RC4 . . . . .	254
7.2.4	Le vecteur d'initialisation . . . . .	255
7.2.5	L'authentification WEP . . . . .	256
7.2.6	Le contrôle d'intégrité. . . . .	257
7.3	Les failles . . . . .	258
7.3.1	Les failles du cryptage . . . . .	258
7.3.2	Les failles de l'authentification . . . . .	263
7.3.3	Les failles du contrôle d'intégrité . . . . .	264
7.4	Résumé . . . . .	266
<b>Chapitre 8 – Le 802.1x . . . . .</b>		<b>269</b>
8.1	L'origine d'EAP . . . . .	270
8.1.1	L'IETF. . . . .	270
8.1.2	Le protocole PPP. . . . .	271
8.1.3	L'authentification avec PPP . . . . .	271
8.2	Le fonctionnement d'EAP . . . . .	273
8.2.1	L'architecture : trois acteurs . . . . .	273
8.2.2	Les dialogues : quatre paquets . . . . .	278
8.2.3	L'EAP et le 802.1x . . . . .	280
8.3	Les méthodes EAP . . . . .	282
8.3.1	EAP/MD5 . . . . .	282
8.3.2	EAP/MS-CHAP-v2 . . . . .	282
8.3.3	EAP/OTP . . . . .	283
8.3.4	EAP/GTC . . . . .	283

8.3.5	EAP/SIM . . . . .	284
8.3.6	EAP/TLS . . . . .	285
8.3.7	EAP/PEAP . . . . .	287
8.3.8	EAP/TTLS . . . . .	289
8.3.9	PEAP ou TTLS ? . . . . .	290
8.3.1	EAP/FAST . . . . .	291
8.3.11	Autres méthodes EAP . . . . .	293
8.4	La sécurité d'EAP . . . . .	293
8.4.1	Les failles . . . . .	293
8.4.2	L'attaque de la méthode EAP . . . . .	294
8.4.3	L'attaque de la session . . . . .	296
8.4.4	Les attaques MiM . . . . .	298
8.4.5	Une bonne sécurité avec le 802.1x . . . . .	301
8.5	Résumé . . . . .	301
<b>Chapitre 9 – WPA et WPA2 . . . . .</b>		<b>303</b>
9.1	Déployer le WPA ou le WPA2 . . . . .	303
9.1.1	Rappels et définitions . . . . .	303
9.1.2	WPA Personal . . . . .	305
9.1.3	WPA Enterprise . . . . .	306
9.2	La distribution des clés . . . . .	309
9.2.1	Une connexion complète . . . . .	309
9.2.2	La hiérarchie des clés . . . . .	311
9.2.3	Dérivation de la clé temporaire PTK . . . . .	314
9.2.4	Rotation de la clé de groupe . . . . .	317
9.2.5	Fonctionnement en mode Ad Hoc . . . . .	318
9.3	La solution TKIP . . . . .	320
9.3.1	Présentation générale . . . . .	320
9.3.2	Le cryptage TKIP . . . . .	321
9.3.3	Empêcher la relecture . . . . .	325
9.3.4	Le contrôle d'intégrité Michael . . . . .	326
9.3.5	Le mode mixte : WEP et WPA . . . . .	328
9.4	La solution AES . . . . .	330
9.4.1	Pourquoi AES ? . . . . .	330
9.4.2	Le WPA/AES . . . . .	330
9.4.3	Les modes de cryptage . . . . .	332
9.4.4	Le CCMP . . . . .	336
9.5	Résumé . . . . .	339

<b>Chapitre 10 – Le RADIUS</b> . . . . .	341
10.1 Les fonctions du serveur RADIUS . . . . .	341
10.1.1 <i>L'authentification</i> . . . . .	341
10.1.2 <i>L'autorisation</i> . . . . .	345
10.1.3 <i>La comptabilisation</i> . . . . .	347
10.2 Le protocole RADIUS . . . . .	350
10.2.1 <i>Le RADIUS et l'UDP</i> . . . . .	350
10.2.2 <i>Six types de paquets</i> . . . . .	352
10.2.3 <i>Le format des paquets RADIUS</i> . . . . .	353
10.2.4 <i>Le 802.1x et le RADIUS</i> . . . . .	356
10.3 Questions de sécurité . . . . .	358
10.3.1 <i>Le secret RADIUS</i> . . . . .	358
10.3.2 <i>L'authenticator</i> . . . . .	358
10.3.3 <i>L'attribut Message-Authenticator</i> . . . . .	362
10.3.4 <i>Attaque hors-ligne contre le secret</i> . . . . .	363
10.3.5 <i>Le RADIUS sur Internet</i> . . . . .	363
10.3.6 <i>Les VLAN</i> . . . . .	368
10.3.7 <i>L'échange de la clé PMK</i> . . . . .	368
10.4 Résumé . . . . .	370
<b>Glossaire</b> . . . . .	373
<b>Sources d'informations complémentaires</b> . . . . .	385
<b>Index</b> . . . . .	389