

# Table des matières

<b>Introduction</b> . . . . .	13
<b>Chapitre 1. L'architecture basée sur l'accès Wi-Fi</b> . . . . .	27
1.1. L'architecture fonctionnelle . . . . .	27
1.1.1. L'architecture basée sur l'interface S2a . . . . .	27
1.1.2. L'architecture basée sur l'interface S2b . . . . .	30
1.1.3. L'architecture basée sur l'interface S2c . . . . .	32
1.2. L'établissement des tunnels . . . . .	33
1.2.1. L'architecture basée sur l'interface S2a . . . . .	33
1.2.1.1. Le mécanisme PMIPv6 . . . . .	34
1.2.1.2. Le mécanisme MIPv4 . . . . .	35
1.2.1.3. Le mécanisme GTPv2 . . . . .	36
1.2.2. L'architecture basée sur l'interface S2b . . . . .	37
1.2.3. L'architecture basée sur l'interface S2c . . . . .	38
1.3. Le protocole DIAMETER . . . . .	40
1.3.1. Les interfaces du serveur AAA . . . . .	40
1.3.2. Les interfaces de l'entité PCRF . . . . .	45
<b>Chapitre 2. La couche MAC</b> . . . . .	47
2.1. La structure des trames . . . . .	47
2.1.1. L'en-tête de la trame de trafic . . . . .	47
2.1.2. La structure des trames de contrôle . . . . .	49
2.1.3. La structure des trames de gestion . . . . .	50
2.2. Les procédures . . . . .	53
2.2.1. Les temporisateurs . . . . .	53
2.2.2. L'enregistrement du mobile . . . . .	54
2.2.3. Le transfert des données . . . . .	55

2.2.4. L'évaluation du canal radioélectrique . . . . .	57
2.2.5. La fragmentation de la trame . . . . .	59
2.2.6. La gestion de la veille . . . . .	59
2.3. La sécurité . . . . .	61
2.3.1. Les mécanismes de sécurité . . . . .	61
2.3.2. Les politiques de sécurité . . . . .	62
2.3.3. L'extension de l'en-tête MAC . . . . .	62
2.3.3.1. Le protocole WEP . . . . .	62
2.3.3.2. Le protocole TKIP . . . . .	64
2.3.3.3. Le protocole CCMP . . . . .	66
2.4. La qualité de service . . . . .	69
2.4.1. Le mécanisme EDCA . . . . .	69
2.4.2. L'impact sur l'en-tête MAC . . . . .	70

**Chapitre 3. Les interfaces 802.11a/g . . . . . 73**

3.1. L'interface 802.11a . . . . .	73
3.1.1. La sous-couche PLCP . . . . .	73
3.1.2. La sous-couche PMD . . . . .	74
3.1.2.1. La chaîne de transmission . . . . .	74
3.1.2.2. L'embrouilleur . . . . .	76
3.1.2.3. Le code de convolution . . . . .	77
3.1.2.4. L'entrelacement . . . . .	77
3.1.2.5. Le schéma de modulation et de codage . . . . .	77
3.1.2.6. La structure du préambule et des symboles OFDM . . . . .	78
3.1.2.7. Le multiplexage OFDM . . . . .	79
3.1.2.8. Le plan de fréquence . . . . .	80
3.2. L'interface 802.11g . . . . .	81
3.2.1. La sous-couche PLCP . . . . .	82
3.2.1.1. Le mode ERP-HR/DSSS . . . . .	82
3.2.1.2. Le mode ERP-OFDM . . . . .	83
3.2.1.3. Le mode DSSS-OFDM . . . . .	84
3.2.2. La sous-couche PMD . . . . .	84

**Chapitre 4. L'interface 802.11n . . . . . 87**

4.1. L'évolution de la couche MAC . . . . .	87
4.1.1. Les trames de gestion . . . . .	88
4.1.1.1. L'élément d'information HT <i>Capabilities</i> . . . . .	88
4.1.1.2. L'élément d'information HT <i>Operation</i> . . . . .	89
4.1.2. La structure de l'en-tête MAC . . . . .	90
4.1.3. L'agrégation des trames . . . . .	91

4.1.3.1. La trame A-MPDU . . . . .	91
4.1.3.2. La trame A-MSDU . . . . .	92
4.1.4. Les trames de contrôle . . . . .	93
4.1.4.1. L'acquittement par bloc . . . . .	93
4.1.4.2. La structure des trames de contrôle . . . . .	94
4.2. La sous-couche PLCP . . . . .	95
4.3. La sous-couche PMD . . . . .	98
4.3.1. La chaîne d'émission . . . . .	98
4.3.2. Le plan de fréquence . . . . .	100
4.3.3. Le multiplexage fréquentiel . . . . .	101
4.3.4. Le multiplexage spatial . . . . .	102
4.3.4.1. Le mécanisme MIMO . . . . .	102
4.3.4.2. Le mécanisme STBC . . . . .	102
4.3.4.3. La formation de faisceaux . . . . .	103
4.3.5. Les schémas de modulation et de codage . . . . .	104
<b>Chapitre 5. L'interface 802.11ac . . . . .</b>	<b>107</b>
5.1. L'évolution de la couche MAC . . . . .	107
5.1.1. Les trames de gestion . . . . .	107
5.1.1.1. L'élément d'information VHT <i>Capabilities</i> . . . . .	107
5.1.1.2. L'élément d'information VHT <i>Operation</i> . . . . .	108
5.1.1.3. L'élément d'information <i>Extended BSS Load</i> . . . . .	109
5.1.1.4. L'élément d'information <i>Wide Bandwidth Channel Switch</i> . . . . .	109
5.1.1.5. L'élément d'information <i>Channel Switch Wrapper</i> . . . . .	110
5.1.1.6. L'élément d'information VHT <i>Transmit Power Envelope</i> . . . . .	110
5.1.1.7. L'élément d'information <i>Quiet Channel</i> . . . . .	110
5.1.1.8. L'élément d'information <i>Operating Mode Notification</i> . . . . .	110
5.1.2. Les trames de contrôle . . . . .	110
5.1.3. La structure de l'en-tête MAC . . . . .	112
5.2. La sous-couche PLCP . . . . .	113
5.3. La sous-couche PMD . . . . .	115
5.3.1. La chaîne d'émission . . . . .	115
5.3.2. Le plan de fréquence . . . . .	120
5.3.3. Le multiplexage fréquentiel . . . . .	122
5.3.4. Le multiplexage spatial . . . . .	122
5.3.5. Les schémas de modulation et de codage . . . . .	123
<b>Chapitre 6. L'authentification mutuelle . . . . .</b>	<b>127</b>
6.1. Le mécanisme 802.1x . . . . .	127
6.1.1. Le protocole EAPOL . . . . .	128

6.1.1.1. Le message EAPOL- <i>Start</i> . . . . .	129
6.1.1.2. Le message EAPOL- <i>Logoff</i> . . . . .	130
6.1.1.3. Le message EAPOL- <i>Key</i> . . . . .	130
6.1.1.4. Le message EAPOL- <i>Encapsulated-ASF-Alert</i> . . . . .	130
6.1.1.5. Le message EAPOL- <i>Announcement</i> . . . . .	130
6.1.1.6. Le message EAPOL- <i>Announcement-Req.</i> . . . . .	130
6.1.2. Le protocole EAP . . . . .	131
6.1.2.1. Le message EAP- <i>Method Identity</i> . . . . .	132
6.1.2.2. Le message EAP- <i>Method Notification</i> . . . . .	132
6.1.2.3. Le message EAP- <i>Method Legacy NAK</i> . . . . .	133
6.1.3. Les messages RADIUS . . . . .	133
6.1.3.1. Le message <i>Access-Request</i> . . . . .	133
6.1.3.2. Le message <i>Access-Challenge</i> . . . . .	133
6.1.3.3. Le message <i>Access-Accept</i> . . . . .	133
6.1.3.4. Le message <i>Access-Reject</i> . . . . .	134
6.1.4. La procédure . . . . .	134
6.2. La gestion des clés. . . . .	135
6.2.1. La hiérarchie des clés. . . . .	135
6.2.2. La procédure <i>4-Way Handshake</i> . . . . .	136
6.2.3. La procédure <i>Group Key Handshake</i> . . . . .	138
6.3. L'application au réseau de mobiles 4G . . . . .	138
6.3.1. La méthode EAP-AKA' . . . . .	138
6.3.2. La procédure d'authentification mutuelle . . . . .	139
6.3.3. La procédure de renouvellement rapide de l'authentification . . . . .	142
6.3.4. L'application au mécanisme MIPv4 FA. . . . .	143

## **Chapitre 7. L'établissement du tunnel SWu . . . . . 145**

7.1. Le mécanisme IPSec . . . . .	145
7.1.1. Les extensions de l'en-tête . . . . .	147
7.1.1.1. L'extension AH. . . . .	147
7.1.1.2. L'extension ESP . . . . .	148
7.1.1.3. Les modes . . . . .	149
7.1.2. Le protocole IKEv2. . . . .	151
7.1.2.1. L'en-tête du message . . . . .	151
7.1.2.2. Les blocs. . . . .	153
7.1.3. La procédure . . . . .	156
7.1.3.1. L'échange IKE_SA_INIT. . . . .	156
7.1.3.2. L'échange IKE_AUTH . . . . .	158
7.1.3.3. L'échange CREATE_CHILD_SA. . . . .	159

7.2. L'application au réseau de mobiles 4G . . . . .	160
7.2.1. La procédure d'établissement du tunnel SWu . . . . .	160
7.2.2. La procédure de renouvellement rapide de l'authentification . . . . .	164

## **Chapitre 8. L'établissement des tunnels S2a/S2b . . . . . 167**

8.1. Le mécanisme PMIPv6 . . . . .	167
8.1.1. L'extension <i>Mobility</i> . . . . .	168
8.1.2. Les procédures. . . . .	169
8.1.2.1. L'attachement du nœud mobile à la fonction LMA. . . . .	169
8.1.2.2. Le changement de fonction MAG . . . . .	170
8.1.3. L'application au réseau de mobiles 4G . . . . .	171
8.1.3.1. L'accès Wi-Fi contrôlé . . . . .	171
8.1.3.2. L'accès Wi-Fi non contrôlé. . . . .	173
8.2. Le mécanisme GTPv2 . . . . .	175
8.2.1. L'accès Wi-Fi contrôlé. . . . .	176
8.2.2. L'accès Wi-Fi non contrôlé . . . . .	177
8.3. Le mécanisme MIPv4 FA . . . . .	177
8.3.1. Les composantes de la mobilité. . . . .	177
8.3.2. La découverte de l'agent étranger . . . . .	178
8.3.3. L'enregistrement . . . . .	179
8.3.4. La procédure . . . . .	179
8.3.5. L'application au réseau de mobiles 4G . . . . .	181

## **Chapitre 9. L'établissement du tunnel S2c . . . . . 185**

9.1. Le mécanisme MIPv6. . . . .	185
9.1.1. Les extensions de l'en-tête IPv6 . . . . .	186
9.1.1.1. L'extension <i>Mobility</i> . . . . .	186
9.1.1.2. L'extension <i>Destination</i> . . . . .	188
9.1.1.3. L'extension <i>Routing</i> . . . . .	188
9.1.2. Les messages ICMPv6 . . . . .	189
9.1.2.1. Le message <i>Home Agent Address Discovery Request</i> . . . . .	189
9.1.2.2. Le message <i>Home Agent Address Discovery Reply</i> . . . . .	189
9.1.2.3. Le message <i>Mobile Prefix Solicitation</i> . . . . .	189
9.1.2.4. Le message <i>Mobile Prefix Advertisement</i> . . . . .	189
9.1.2.5. Les modifications du protocole ND . . . . .	189
9.1.3. Les procédures. . . . .	190
9.1.3.1. L'attachement du nœud mobile à l'agent hôte. . . . .	190
9.1.3.2. Le transfert des données. . . . .	191
9.1.3.3. Le changement de réseau local. . . . .	193

9.1.3.4. Le retour du nœud mobile au réseau hôte . . . . .	194
9.1.3.5. La procédure <i>Return Routability</i> . . . . .	195
9.2. Le mécanisme DSMIPv6 . . . . .	196
9.3. L'application au réseau de mobiles 4G . . . . .	197
9.3.1. L'accès Wi-Fi contrôlé . . . . .	197
9.3.2. L'accès Wi-Fi non contrôlé . . . . .	198
9.3.3. La fonction IFOM . . . . .	199

**Chapitre 10. La découverte et la sélection du réseau . . . . . 201**

10.1. Les mécanismes définis par l'organisme 3GPP . . . . .	201
10.1.1. La fonction ANDSF . . . . .	201
10.1.1.1. Les informations ANDI . . . . .	202
10.1.1.2. La politique ISMP . . . . .	202
10.1.1.3. Les règles ISRP . . . . .	204
10.1.1.4. Les règles IARP . . . . .	206
10.1.1.5. La politique WLANSP . . . . .	207
10.1.1.6. Les préférences du réseau d'accès Wi-Fi . . . . .	208
10.1.2. L'assistance du réseau RAN . . . . .	209
10.2. Les mécanismes définis par les organismes IEEE et WFA . . . . .	210
10.2.1. Les éléments d'information fournis par la balise . . . . .	212
10.2.1.1. L'élément HESSID . . . . .	212
10.2.1.2. Le champ <i>Access Network Type</i> . . . . .	212
10.2.1.3. Le champ <i>Internet Available</i> . . . . .	212
10.2.1.4. L'élément <i>BSS Load</i> . . . . .	212
10.2.2. Les éléments d'information fournis par le serveur ANQP . . . . .	213
10.2.2.1. L'élément <i>3GPP Cellular Network</i> . . . . .	213
10.2.2.2. L'élément <i>NAI Realm</i> . . . . .	213
10.2.2.3. L'élément <i>Roaming Consortium</i> . . . . .	213
10.2.2.4. L'élément <i>Domain Name</i> . . . . .	213
10.2.2.5. L'élément <i>Venue Name</i> . . . . .	214
10.2.2.6. L'élément <i>Operator's Friendly Name</i> . . . . .	214
10.2.2.7. L'élément <i>IP Address Type Availability</i> . . . . .	214
10.2.2.8. L'élément <i>WAN Metrics</i> . . . . .	214
10.2.2.9. L'élément <i>Connection Capability</i> . . . . .	214
10.2.2.10. L'élément <i>Operating Class Indication</i> . . . . .	215
10.2.2.11. L'élément <i>Network Authentication Type</i> . . . . .	215
10.2.2.12. L'élément <i>OSU Providers List</i> . . . . .	215
10.2.2.13. L'élément <i>Icon Request &amp; Response</i> . . . . .	215
10.2.2.14. L'élément <i>HS Query List</i> . . . . .	216
10.2.2.15. L'élément <i>HS Capability List</i> . . . . .	216
10.2.2.16. L'élément <i>NAI Home Realm Query</i> . . . . .	216

---

<b>Chapitre 11. L'agrégation des canaux.</b> . . . . .	<b>217</b>
11.1. L'architecture fonctionnelle . . . . .	217
11.2. L'architecture protocolaire . . . . .	218
11.2.1. L'agrégation LWA . . . . .	218
11.2.2. L'agrégation LWIP . . . . .	221
11.2.3. L'agrégation LAA. . . . .	222
11.3. Les procédures . . . . .	222
11.3.1. L'agrégation LWA . . . . .	222
11.3.1.1. La procédure WT Addition . . . . .	222
11.3.1.2. La procédure WT Modification. . . . .	223
11.3.1.3. La procédure WT Release . . . . .	225
11.3.2. L'agrégation LWIP . . . . .	226
11.3.3. L'agrégation LAA. . . . .	228
11.4. Le protocole PDCP . . . . .	229
<b>Chapitre 12. L'agrégation MPTCP</b> . . . . .	<b>233</b>
12.1. L'architecture fonctionnelle . . . . .	233
12.2. Le protocole TCP . . . . .	234
12.2.1. L'en-tête TCP . . . . .	234
12.2.2. L'établissement et la fermeture de la connexion . . . . .	236
12.2.3. Le transfert des données . . . . .	236
12.2.4. Les mécanismes <i>Slow Start</i> et <i>Congestion Avoidance</i> . . . . .	237
12.2.5. Les mécanismes <i>Fast Retransmit</i> et <i>Fast Recovery</i> . . . . .	238
12.2.6. Le mécanisme ECN. . . . .	239
12.3. Le protocole MPTCP . . . . .	241
12.3.1. L'établissement de la connexion MPTCP . . . . .	242
12.3.2. L'ajout d'une connexion TCP . . . . .	243
12.3.3. Le transfert des données . . . . .	245
12.3.4. La fermeture de la connexion MPTCP. . . . .	246
12.3.5. L'ajout et le retrait d'adresse . . . . .	248
12.3.6. Le retour à la connexion TCP . . . . .	249
<b>Liste des abréviations</b> . . . . .	<b>251</b>
<b>Bibliographie</b> . . . . .	<b>261</b>
<b>Index</b> . . . . .	<b>265</b>