Le roaming dans le wifi

Kévin DENIS,

Etude réalisée début 2007

Table des matières

1.Définition du sujet 3
1.Qu'est ce que le wifi 3
1.Le mode ad-hoc 3
2.Le mode infrastructure 3
3.Connexion à un reseau Wi-Fi en mode infrastructure. 5
2.Qu'est ce que le roaming en wifi? 5
3.Pourquoi le wifi n'implémente pas directement le roaming? 5
1.Cas laissé "ouvert" par la norme 5
2.Solutions propriétaires et normalisation. 6
4.Dans quel cadre allons nous étudier le roaming dans le wifi? 6
1.Le mode infrastructure 6
2.Le roaming niveau L2 6
3.Le roaming niveau L3 n'est pas abordé. 6
4.Quel protocole expérimental utiliser? 6
5.Quels besoins technologiques sont à l'origine du développement du roaming dans le wifi? 7
1.Généralisation des bornes wifi 7
2.La VoIP et ses contraintes 7

2.La norme 802.11F ou IAPP (Inter Access Point Protocol) 8
1.Lien entre 802.11F et IAPP 8
2.Cadre technique choisi par l'IEEE pour développer 802.11F 8
3.Fonctionnement de 802.11F 9
4.Les raisons de l'échec de la norme 802.11F 11
1.Lenteur du roaming 11
2.Non aboutissement des normes additionnelles. 12
3.Désinterêt de la part des développeurs. 12
5.La mise à la retraite de la norme en 2006 par l'IEEE 13

3.Le roaming poussé par les solutions propriétaires et 802.11i 15
1.L'arrivée de 802.11i (WPA2) pour des raisons de sécurité 15
2.802.11i va faciliter le roaming avec l'aide de solutions propriétaires 15
1.Les apports de 802.11i 15
2.Les solutions propriétaires 16
3.Un comparatif de quatres solutions 17

4.Conclusion 18
1.L'obligation de choisir un constructeur pour roamer 18
2.Vers la convergence wifi / GSM? 18

Références 19

1. Définition du sujet

Ce chapitre introduit quelques rappels sur le wifi nécessaires à la compréhension du sujet, puis définit le concept du roaming et cerne le cadre technique dans lequel le roaming sera étudié.

1. Qu'est ce que le wifi

Le Wi-Fi est une technologie de réseau informatique sans fil. Il est basé sur la norme IEEE 802.11 (ISO/CEI 8802-11). Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fil. Dans la pratique, le Wi-Fi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) ou même des périphériques à une liaison haut débit (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) [1].

Le Wi-Fi offre deux solutions possibles pour connecter des ordinateurs en réseau : le mode Infrastructure et le mode Ad-Hoc [2].

1. Le mode ad-hoc

Les équipements communiquent entre eux directement sans intermédiaire. Les informations nécessaires à la création d'un réseau ad-hoc sont les suivantes: le SSID (Service Set Identifier), ou nom du réseau Wi-Fi, le canal utilisé de 1 à 13, qui correspond à la fréquence d'émission, la méthode de chiffrement des données, et éventuellement le mot de passe.

2. Le mode infrastructure

Cest le mode le plus courant pour créer un réseau Wi-Fi. Les informations nécessaires à la création d'un réseau Infrastructure sont identiques au mode Ad-Hoc. En mode Infrastructure, les ordinateurs se connectent entre eux par l'intermédiaire d'une borne d'accès centrale, le point d'accès ou AP (Access Point). Il est important de noter que toutes les communications passeront par ce point central, même en cas de liaisons entre deux stations.

Autrement dit, le mode infrastructure correspond à des stations Wi-Fi fédérées autour d'un AP et partageant un SSID commun. Il est possible d'utiliser plusieurs AP reliés entre eux par un système de distribution. La compréhension de cette définition nécessite de détailler plusieurs termes qui sont utilisés:

-SSID : Service Set Identifier. Le SSID est un code envoyé avec toutes les trames Wi-FI à des fins d'identification. Ainsi, deux réseaux différents peuvent partager la même fréquence, s'ils n'ont pas le même SSID. C'est une chaîne de caractères. Deux

équipements qui souhaitent communiquer doivent absolument avoir le même SSID.

-BSS : Basic Service Set. Cela peut être vu comme la zone couverte par le signal d'un point d'accès (AP). Toutes les stations se trouvant dans la zone géographique d'un BSS peuvent émettre et recevoir des trames de l'AP.

-Beacon : balise. C'est une trame envoyée régulièrement par l'AP pour signaler sa présence. Cela fonctionne sur le même principe que les radio-balises en aviation. Les stations ont libre latitude sur la manière dont traiter l'information contenue dans ce beacon. En d'autres termes, tout point situé dans le BSS reçoit le beacon à intervalle régulier.

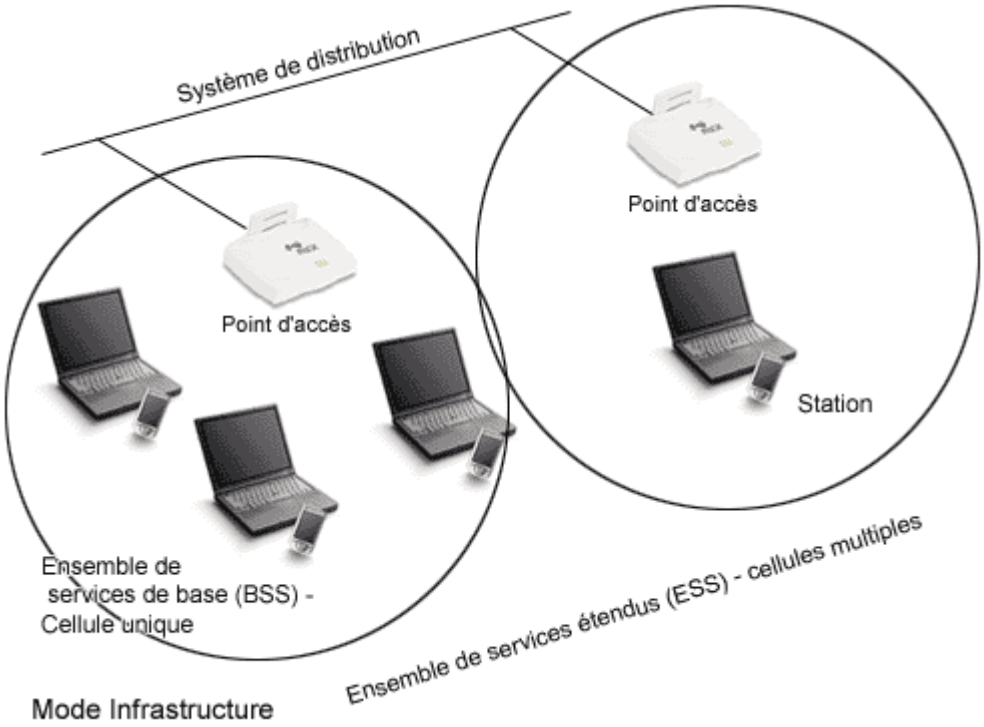
-BSSID : Basic Service Set IDentifier. A ne pas confondre avec le SSID. Le BSSID correspond à l'adresse MAC de l'équipement Wi-FI, et de fait, est un identifiant unique.

-ESS : Extended Service Set. Un ESS correspond à la réunion de plusieurs BSS qui sont reliés par un lien réseau (wifi ou filaire) et qui partagent le même SSID. Il est nécessaire de remarquer qu'ils n'ont pas à partager la même fréquence, c'est le SSID seul qui spécifie l'appartenance au même réseau.

-DS : Distribution System. C'est le lien réseau qui permet aux AP de communiquer entre eux. Généralement filaire, la littérature indique que l'on peut construire un DS également sur du Wi-Fi.

-STA : station. Cela correspond à tout matériel équipé d'une carte Wi-FI autre qu'un AP. Il peut s'agir d'un PC avec une antenne wifi, mais également des PDA, des téléphones wifi, ou de tout autre type d'équipement.

Voici un schéma représentant en situation l'ensemble des notions définies ci-dessus:



Un ESS, deux AP et des stations

3. Connexion à un reseau Wi-Fi en mode infrastructure.

La connexion d'une station à un AP s'effectue en deux phases. La première correspond à une phase d'authentification, la seconde à l'association.

Authentification: La station désirant entrer sur le réseau Wi-Fi doit s'authentifier sur l'AP. Si le réseau est ouvert, cette phase est obligatoirement un succès. Les mécanismes actuels demandent un mot de passe, voire différents challenges pour s'authentifier sur un AP. Une littérature abondante existe sur ce sujet. Voir les défauts du WEP, le WPA et le WPA2.

Association: Une fois authentifiée, une station est associée et peut commencer à émettre des trames sur le réseau. L'AP relaiera ces informations aux destinataires concernés.

2. Qu'est ce que le roaming en wifi?

Le roaming, ou handover, ou encore appelé l'itinérance en wifi représente l'action qui consiste pour une station à changer de point d'accès (AP) sans perdre sa connectivité réseau.

Cette définition va servir de fil directeur tout au long de cet exposé.

Attention toutefois, dans les réseaux GSM, les notions de roaming et de handover représentent des actions différentes, ce qui n'est pas le cas dans le wifi. Les mots "roaming", "handover", ou "itinérance" seront donc utilisés indifféremment tout au long de ce document.

3. Pourquoi le wifi n'implémente pas directement le roaming?

Le roaming n'a pas été implémenté dans la norme Wi-Fi bien que cette dernière soit une technologie sans fil, ce qui a laissé le champ libre à des implémentations soit normalisées, soit propriétaires.

1. Cas laissé "ouvert" par la norme

Le wifi existe depuis 1999. A cette date la notion de sans fil existe pour les stations portables. Mais un ordinateur portable ne se déplace que lorsqu'il est éteint, une fois allumé il reste fixe. Contrairement au réseau GSM qui dès le début a pensé à introduire les notions d'itinérance, le wifi a laissé cette option de côté. Le roaming est donc absent de la norme Wi-Fi 802.11. Ce cas d'utilisation a été délibérement laissé ouvert, afin de permettre à des solutions futures d'impléménter le roaming en cas de besoin.

2. Solutions propriétaires et normalisation.

Certains constructeurs ont tenté de mettre en place le roaming via des solutions propriétaires. La première s'est appellée IAPP pour Inter Access Point Protocol. Sur les bases d'IAPP, l'IEEE a aboutit en 2003 à la rédaction d'un "*trial and use*", qu'on pourrait traduire par "recommandations d'usage" qui présente la norme 802.11F. Malgré la création de cette norme, les constructeurs ont continué d'implémenter leur propres méthodes permettant le roaming de stations dans les réseaux wifi.

4. Dans quel cadre allons nous étudier le roaming dans le wifi?

Il existe une multitude de façons de roamer dans un réseau wifi. Nous nous centrerons sur les réseaux Wi-Fi en mode infrastructure, sans nous intéresser au contenu des échanges.

1. Le mode infrastructure

Du fait même de la définition citée plus haut, "changement de point d'accès", cet exposé traitera du roaming uniquement dans les réseaux disposants de points d'accès, c'est à dire le mode infrastructure. Il existe des méthodes d'itinérance dans les réseaux ad-hoc. Ces méthodes ne sont pas étudiées ici.

2. Le roaming niveau L2

Cet exposé parle du roaming niveau L2. C'est à dire qu'il va traiter du niveau liaison de données. C'est une stricte application de la définition citée plus haut: cela consiste à changer de point d'accès sans perdre sa connectivité réseau. Le contenu des échanges réseaux ne sera pas étudié.

3. Le roaming niveau L3 n'est pas abordé.

Le roaming inclut un déplacement, il est tout à fait concevable d'imaginer lors d'un déplacement de se retrouver sur un autre réseau IP que celui d'origine. IP propose plusieurs mécanismes pour pallier ce problème (renouvellement DHCP, mobile IP...), mécanismes qui dépassent le simple fait du roaming wifi et qui ne seront pas traités ici.

4. Quel protocole expérimental utiliser?

Il n'existe pas de protocole expérimental clairement défini pour étudier le roaming. La première méthode consiste à se déplacer physiquement avec une station et de se mouvoir entre deux AP. Cette méthode est par exemple utilisée lors des tests effectués par "groupe tests" (laboratoire de mesures d'équipements informatiques) dont les résultats sont donnés plus bas. Il existe une autre méthode plus judicieuse qui permet de réaliser un très grand nombre de répétitions du test.

Cette méthode s'appuye sur le fait qu'il est possible de moduler la puissance d'émission des antennes des AP. Le protocole expérimental consiste à fixer une station et deux AP.

AP --- STA --- AP

L'AP de gauche délivre une puissance de 15mW et l'AP de droite une puissance de 5mW. L'idée consiste à diminuer la puissance de l'AP de gauche et augmenter la puissance de l'AP de droite. Cela simulera pour la station le fait qu'elle se déplace et s'approche de l'AP de droite, la forçant ainsi à roamer. L'opération peut être ensuite réalisée dans l'autre sens. L'avantage de cette solution est de pouvoir répéter les opérations de test un très grand nombre de fois. De la même manière, en installant une station au centre d'un cercle d'AP, il est possible de simuler un roaming successif.

5. Quels besoins technologiques sont à l'origine du développement du roaming dans le wifi?

Le roaming n'a donc pas été initialement prévu dans le wifi. Ce point soulève une question: Quel besoin technologique a finalement poussé le développement de solutions permettant le roaming de stations dans un réseau Wi-Fi infrastructure?

1. Généralisation des bornes wifi

A l'origine, les équipements Wi-Fi, spécialement les AP, étaient du matériel coûteux, et assez peu diffusé. De ce fait, il était extrêmement rare de trouver des réseaux avec plusieurs AP et donc les besoins en roaming étaient très peu répandus. Aujourd'hui, du fait des avantages et de la baisse des couts des réseaux sans fils, les entreprises tendent à vouloir couvrir l'ensemble de leurs locaux en Wi-Fi. Cela pose le problème de passer d'un AP à un autre sans perte de connectivité réseau.

Même si plusieurs champs d'applications supportent facilement des déconnexions / reconnexions réseau (comme la consultation de pages web sur internet ou la déconnexion / reconnexion peut se faire entre deux pages), il en est une qui ne peut pas se le permettre: la VoIP (voix sur IP) [11].

2. La VoIP et ses contraintes

L'arrivée de la VoIP et du développement du wifi génèrent notamment la nécessité de disposer d'un roaming efficace. En effet la principale contrainte de la VoIP est la continuité du débit afin qu'il n'y ait pas de rupture dans la conversation. Ainsi, pour tout délai supérieur à 50 ms lors de la transmission des données, l'oreille perçoit nettement la coupure. Dès lors, l'application VoIP apparaît comme l'application candidate idéale pour valider le fonctionnement du roaming en Wi-Fi. De plus, la VoIP est une des premières cibles du roaming, l'utilisateur est en déplacement et a besoin d'un flux continu. Enfin, si la VoIP fonctionne, toute autre application nécessitant le roaming en Wi-Fi fonctionnera. C'est la raison pour laquelle la VoIP sera l'application étalon pour mesurer la validité d'une solution de roaming.

Par ailleurs, pour toute application nécessitant des délais de transmissions de données inférieurs à 50 ms, c'est le choix même du Wi-Fi qui est discutable, compte tenu des délais aléatoires de transmissions.

2. La norme 802.11F ou IAPP (Inter Access Point Protocol)

Ce chapitre traitera de la norme 802.11F, de l'explication technique de son fonctionnement et des raisons de son échec.

1. Lien entre 802.11F et IAPP

L'IEEE s'est inspiré d'IAPP pour développer sa norme. C'est pour cette raison que l'acronyme IAPP reste encore très présent dans la littérature et les programmes associés. Les termes IAPP et 802.11F [3] ont fini par devenir équivalents.

Comme IAPP, 802.11F est un protocole utilisé pour le management d'un ESS qui définit les communications nécessaires à réaliser entre les AP pour son bon fonctionnement. Ce protocole a besoin d'un système de distribution (DS) pour échanger les informations entre les AP. Enfin, notons qu'il est possible d'adjoindre un ou plusieurs serveurs RADIUS qui permettront deux choses: en premier lieu, d'associer chaque AP avec son BSSID et permettre la consultation de cette information, et en second lieu de donner des clés de cryptages aux AP pour augmenter la confidentialité des échanges. Ces deux fonctions sont entièrement facultatives et laissées à la discrétion du logiciel implémentant 802.11F [4].

2. Cadre technique choisi par l'IEEE pour développer 802.11F

L'IEEE a encadré de manière formelle la mise en oeuvre du roaming dans le Wi-Fi pour la norme 802.11F. Cette norme répond à un cahier des charges qui définit un certain nombre de contraintes techniques, un environnement matériel précis, ainsi que deux prérequis logiciels pour la réalisation du roaming.

Premièrement, les contraintes sont les suivantes:

Ouverture. Du fait de sa publication par l'IEEE, cette norme est ouverte, librement consultable et librement implémentable.

Interopérabilite multi constructeurs. Un des buts de cette ouverture est de pouvoir mélanger différents matériels de différents équipementiers, c'est à dire l'interopérabilité.

Absence de point central: il n'y a aucun management centralisé. Il n'a pas été choisi d'"élire" un AP pour le dédier à un rôle particulier comme fédérateur, ou centralisateur d'informations comme cela peut-être vu dans d'autres protocoles. Tous les AP sont égaux en fonctions et possibilités. Ce choix a des conséquences importantes qui sont

étudiées ultérieurement.

Independance du contenu: Tout d'abord, la norme reste centrée sur le Level 2, c'est-à-dire le niveau liaison de données. Toute latitude est laissée quant au contenu des données transmises. Ainsi peuvent circuler de l'IP, de l'appletalk ou tout autre protocole. Ensuite, IAPP n'est pas un protocole de routage, c'est donc aux couches supérieures de s'assurer que l'information arrive. IP devra mettre en oeuvre des mécanismes de renouvellement de baux DHCP ou mobile IP, mais ces cas ne seront pas traités ici.

Neutralité des stations: La norme 802.11F ne concerne que les points d'accès. Sa mise en oeuvre suppose que les stations ne doivent subir aucune modification, ni logicielle, ni matérielle.

Deuxièmement l'environnement logiciel nécessite l'emploi d'un ou plusieurs AP, d'une ou plusieurs stations, d'un système de distributions inter-AP (généralement ethernet, bien qu'un système de distribution wifi puisse être envisagé), et de zéro ou plus serveurs RADIUS.

Troisièmement, pour le bon fonctionnement de 802.11F il est nécessaire que les deux conditions suivantes soient remplies:

-D'une part 802.11F se base sur le fait qu'une station envoie une trame de réassociation plutôt que d'association lors de la connexion sur un nouvel AP. 802.11F ne travaillant qu'au niveau AP, il lui faut savoir si la station se connecte sur la réseau pour la première fois ou s'il s'agit d'une station qui se déplace.

-D'autre part, les AP doivent surveiller en permanence l'accès au système de distribution. En cas de perte de connectivité, ils doivent stopper globalement toute activité réseau en attente du retour de la connectivité.

3. Fonctionnement de 802.11F

802.11F implémente trois types d'échanges de messages:

-Arrivée d'une station dans l'ESS

Un AP doit communiquer en multicast chaque nouvelle assocation de station. Les autres AP doivent maintenir à jour une table de correspondance AP <-> station.

-Déplacement d'une station dans l'ESS

Lors d'un déplacement, la station envoie une trame de réassociation. L'AP joint envoie à l'ancien une requête lui signalant que cette station vient de se connecter à lui. L'ancien AP lui envoie le cas échéant le contexte réseau non encore transmis à la station au nouvel AP pour le transférer.

-Demande de notification de cache

Il est possible d'implémenter un système de reconnaissance géographique entre les AP et les stations qui se déplacent afin de prévoir vers quels AP une station est susceptible de se déplacer. Une fois cette carte construite, un AP peut demander à ses proches voisins les contextes réseaux des autres stations afin de pouvoir

accélerer le roaming le cas échéant.

Ces trois échanges reposent sur cinq services IAPP: IAPP-INITIATE, IAPP-TERMINATE, IAPP-ADD, IAPP-MOVE et IAPP-CACHE-NOTIFY. Les fonctions associées à ces services sont: *request*, *confirm*, *indication* et *response*, ci-après évoqués plus en détail.

Pour la construction d'un ESS, trois services sont nécessaires. Ces services vont normaliser les échanges entre les AP qui permettent d'élaborer l'ESS et de le faire évoluer au cours du temps. Pour entrer dans un ESS, un AP ne doit être associé avec aucune station.

-IAPP-INITIATE. Ce service accepte deux fonctions: *request* et *confirm*. Le *request* correspond à l'entrée d'un AP dans l'ESS. Les informations communiquées sont le protocole (TCP ou UDP), le port nécessaire à la communication en multicast entre les AP, et éventuellement l'identification du serveur RADIUS s'il existe. Un service correspondant sur le port donné doit être démarré. Le *confirm* doit être remonté avec un status SUCCESS ou FAILED.

-IAPP-TERMINATE. A l'inverse, ce service correspond à la sortie d'un AP d'un ESS et signifie l'arrêt de toute opération IAPP. Entre autre l'arrêt du service sur le port TCP ou UDP, et l'arrêt de tout type de trafic IAPP, ainsi que la déconnexion de toutes les stations.

-IAPP-ADD. Ce service va correspondre à l'arrivée d'une station. Cela peut être vu comme l'allumage d'une station, ou son arrivée dans la zone d'influence d'un des BSS de l'ESS. La fonction *request*, est envoyée lors de l'arrivée d'une station dans l'ESS. Ce service est utilisé lorsqu'un AP reçoit une requête d'association de la part d'une station. Concrètement, l'AP envoie en broadcast l'information selon laquelle cette station (en se basant sur son BSSID) s'est connectée sur lui. Les autres AP et équipements réseaux peuvent mettre à jour leurs tables d'associations. Cette fonction est complétée par *confirm*, qui indique à l'AP si le request s'est correctement terminé. Enfin, il existe également la fonction *indication* qui est envoyée par un AP en réponse à un *request* pour signaler qu'il est déjà associé avec la station en question. Un algorithme permet de savoir avec quel AP la station doit continuer la connexion.

Ainsi, l'ESS est construit avec les IAPP-INITIATE, des stations sont entrées dans cet ESS avec des IAPP-ADD, elles peuvent maintenant se déplacer à l'aide d'IAPP-ADD.

-IAPP-MOVE. La première fonction *request*, est envoyée par un AP lorsqu'il reçoit une trame de réassociation de la part d'une station. Cette information est envoyée à l'ancien AP avec lequel la station était précedemment connectée (information connue à l'aide de l'IAPP-ADD envoyé par l'AP lors de la précédente connexion de la station). La fonction *confirm* contient notamment le contexte 802.11 éventuel envoyé par l'ancien AP correspondant à cette station. Si cette réassociation est réussie, alors l'AP envoie un *indication* pour signaler à l'ensemble de l'ESS que la station s'est connectée avec lui. Et enfin, la fonction *response* correspond à l'envoi par l'ancien AP au nouvel AP de tout le contexte réseau hors 802.11 qui concerne la station.

Enfin, IAPP peut mettre en oeuvre un mécanisme de cache.

-IAPP-CACHE-NOTIFY: Cette primitive n'a pas obligatoirement vocation à être

implémentée. Cela permet aux AP de gérer des caches de contextes réseaux, une fois qu'ils ont appris la géographie interne des stations et de leurs positions et de leurs mouvements respectifs. La fonction *request* signale à tous les voisins connus que la station vient de se connecter. Cette fonction est suivie d'une fonction *confirm* dont le rôle est de donner le statut de la fonction *request* qui se traduit par une réussite ou un échec. Enfin, la fonction indication est reçue par un AP voisin et contient le contexte réseau à mettre en cache au cas où la station viendrait à se connecter. Et la fonction *response* permet de donner le statut de la fonction *indication*.

Ces fonctions permettent d'effectuer le roaming des stations dans un ESS. Le traitement des erreurs (timeout, échec d'authentification, etc..) n'a pas été abordé ici sachant que tous ces éléments sont traités par la norme.

Par ailleurs il est important de faire deux remarques sur la mise en oeuvre pratique de cette norme. D'une part, l'accent a été porté sur la mise en cache et la diffusion du contexte réseau, afin d'améliorer le temps mis par le roaming. Cela nécessitera d'étudier si la mise en cache du contexte réseau est une stratégie qui permet d'améliorer efficacement les performances.

D'autre part, le contexte réseau est une notion qui est abstarite. La norme ne traite que du niveau 2, liaison de données, elle prend le parti de ne pas définir ce contexte réseau qui concerne les couches supérieures. Mais concrètement, il apparaît difficile de comprendre ce qui pourrait être sous entendu par "contexte réseau" dans un réseau IP. Ce point n'est pas abordé et laissé à la discrétion du programmeur implémentant la norme.

4. Les raisons de l'échec de la norme 802.11F

La norme 802.11F a été un échec. Différentes causes peuvent l'expliquer. Premièrement, le roaming, bien que fonctionnel, est très lent. Deuxièmement, deux normes additionnelles qui devaient améliorer le roaming n'ont jamais vu le jour. Troisièmement, sans doute du fait des deux premiers points, la norme 802.11F a souffert d'un certains désinterêt de la part des acteurs du marché, tant dans le logiciel libre que dans le logiciel propriétaire.

1. Lenteur du roaming

Tous les tests effectués et diffusés sur internet montrent des temps de roaming avec 802.11F extrêmement longs. Cela dépasse les centaines de millisecondes, quelquefois la seconde, voire même plusieurs secondes [12]. Dans ce cas, la VoIP utilisée comme étalon est totalement inefficace.

De plus, avec des temps supérieurs à 2s pour roamer, on dépasse les délais de timeouts TCP qui pourront poser des problèmes de duplications de trames lors de la reconnexion.

Enfin, il est quasi-systématiquement plus rapide de se déconnecter et se reconnecter du réseau Wi-Fi plutôt que d'utiliser le roaming proposé par 802.11F, ce qui est presque

paradoxal.

Afin d'analyser cette lenteur, des études ont été réalisées pour mesurer précisement chacune des étapes du roaming et définir ainsi celles qui prenaient le plus de temps. Le point de lenteur le plus tangible correspond à la réauthentification auprès de l'AP destination. En effet, durant cet échange, le trafic est coupé depuis l'ancien AP jusqu'à ce que la station se soit réauthentifiée et réassociée. Cela est dû au processus d'authentification qui s'effectue selon le mode de sécurité choisi, WEP (3-way handshake) ou WPA (4-way handshake). Ces poignées de main prennent du temps et influent fortement sur les mauvais résultats du temps de roaming.

Comme vu précédemment, l'accent a plutôt été mis sur le phénomène de mise en cache du contexte réseau et la norme 802.11F ne donne aucune précisions sur le mécanisme d'authentification et sur les manières de l'accélérer.

2. Non aboutissement des normes additionnelles.

L'IEEE a travaillé sur deux normes, la 802.11k [5] et la 802.11r [6] qui devaient améliorer globalement le mécanisme de roaming, sans qu'elles aboutissent.

Revenons sur le fonctionnement de la norme 802.11F. Théoriquement, c'est la station qui choisit le point d'accès sur lequel elle veut se connecter. Le choix s'effectue à partir de la puissance d'émission ce qui signifie de manière générale l'AP le plus proche. Mais l'AP le plus proche n'est pas forcément le choix le plus judicieux. Les AP peuvent être reliés de différentes manières au Distribution System, certains liens pouvant répondre à certains type de trafic, d'autre non. Un AP peut par exemple être relativement surchargé, alors qu'un autre situé plus loin sera complètement libre. Pour pallier ce défaut, l'IEEE a réfléchi sur la norme 802.11k qui devait servir à mesurer la qualité de connexion selon plusieurs critères. Cette norme et ces critères n'ont toujours pas été ratifiés.

L'IEEE a également travaillé sur une norme 802.11r appelée "fast roaming". Cette norme n'a toujours pas été ratifiée non plus.

A ce jour, les processus d'amélioration de 802.11F sont au point mort.

3. Désinterêt de la part des développeurs.

Enfin, le déploiement de cette norme est très faible. Il ne s'est produit aucune dynamique de déploiement massif, de documentations et d'implémentations.

A titre d'exemple, Futsoft vend une pile 802.11F portable. Son site web renvoie vers des pages inexistantes, et les mails que je leur ai envoyé afin d'obtenir des précisions techniques sont restés sans réponse. Dans le logiciel libre, deux projets différents ayant le même nom existent: hostapd sous linux [9] et hostapd sous openBSD [10]. Dans les deux programmes, la norme n'est pas entièrement implémentée; par exemple les interactions avec Radius ne sont pas gérées avec linux, et la version openBSD ne gère pas les stations en DHCP. De même, les développeurs respectifs de ces projets n'ont pas pris

le temps de répondre à mes mails de demande d'explications sur les aspects techniques de 802.11F et sur le caractère incomplet de leur implémentation.

Enfin, la littérature sur internet concernant la norme 802.11F est très pauvre, traduisant le manque d'interêt des utilisateurs ou concepteurs de réseaux Wi-Fi dans cette norme.

Pour les implémentations propriétaires, il est possible d'imaginer la mauvaise volonté manifeste des constructeurs de vendre des solutions interopérables. Cisco propose depuis très longtemps de la VoIP sur wifi, mais uniquement avec ses points d'accès et sa technologie. Effectivement, pour un constructeur, le fait de vendre une solution d'infrastructure wifi non-interopérable est d'un interêt financier certain.

Toutes ces raisons mènent à l'abandon progressif et au désinterêt croissant de tous les acteurs susceptibles d'apporter des améliorations à la norme 802.11F.

5. La mise à la retraite de la norme en 2006 par l'IEEE

Au vu des ces conclusions, temps de roaming trop lent, ininterêt de la part des développeurs et constructeurs, absence d'amélioration, le roaming avec 802.11F semble être une technologie inefficace.

Dès 2004, le développeur principal d'hostapd (linux), répondait à la question de la perennité de cette norme 802.11F. (source http://lists.shmoo.com/pipermail/hostap/2004-October/008206.html):

> Or, as a very basic question: is IAPP slowly dying?
IEEE 802.11F-2003 is trial-use recommended practice, not amendment to IEEE 802.11 standard. It will expire next summer if it is not revised and I haven't really noticed much activity within IEEE 802.11 working group to do anything about this. In other words, I'm not too surprised if it ends up going the way of dodo..
I can see some uses for the current IAPP, mainly the IAPP ADD-notify (and MOVE-notify/response to some extent) to clear old association data from APs. However, further use for IEEE 802.11, like context transfer, is quite open. IEEE 802.11F-2003 itself does not specify what kind of context would be transferred, it just provides a mechanism for transferring such data..
I haven't seen concrete plans on what people would like to do with IAPP. If someone has one, it would be interesting to get some details (e.g., what problem is being solved, what context data is transferred, etc.).

Dans ce contexte, l'IEEE a donc décidé en mai 2006 de mettre à la retraite cette norme.

http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

"[Administratively Withdrawn by IEEE-SA Standards Board on 02/03/06]"

Comme nous le voyons, le Wi-Fi a implémenté le roaming à l'aide de la norme 802.11F, mais cette norme n'a jamais vraiment percé. Cependant l'échec de cette norme n'a pas pour corollaire l'abandon du roaming en wifi.

3. Le roaming poussé par les solutions propriétaires et 802.11i

Le roaming est rendu possible grace à des implémentations propriétaires.

1. L'arrivée de 802.11i (WPA2) pour des raisons de sécurité

Pour comprendre l'arrivée de la norme 802.11i et de son interêt vis a vis du roaming en wifi, il faut effectuer un bref retour sur les mécanismes de sécurité implémentés en wifi.

Pour communiquer sur un réseau wifi, une station doit s'authentifier puis s'associer. L'authentification peut se réaliser de plusieurs manières.

Open : n'implique aucun mécanisme de sécurité. Toute station passant à proximité d'une autre station ou d'un autre AP peut s'associer. Cette méthode de fonctionnement est à éviter car elle rend vulnérable le réseau.

WEP : A l'origine prévue pour garantir de la confidentialité sur les réseaux wifi (WEP signifie Wired Equivalent Privacy) cette norme de sécurité a été cassée [14], à la fois théoriquement et pratiquement. Cette norme est à abandonner.

WPA : face à l'échec du WEP, la wifi Alliance a décide de promouvoir le WPA qui couvrait la majorité des failles du WEP. Un des critère pour la mise en place WPA était qu'il devait fonctionner sur le même hardware que les puces réalisant le WEP.

WPA2 : enfin, la norme 802.11i implémente le WPA2 qui apporte un niveau de sécurité satisfaisant. WPA2 demande un nouveau hardware. Depuis 2002, toutes les puces wifi doivent supporter le WPA2.

Cette norme 802.11i a été majoritairement poussée à sortir pour des raisons de sécurité, mais l'IEEE a profité de l'évolution de la norme pour ajouter des possibilités, dont la mise en cache des clés de sessions qui va directement influer sur la facilitation du roaming.

2. 802.11i va faciliter le roaming avec l'aide de solutions propriétaires

1. Les apports de 802.11i

Pour expliquer l'apport de 802.11i et de la mise en cache des clés de sessions, il faut revenir sur les mécanismes entrant en jeu lors d'une authentification. L'AP et la station négocient ensemble une clé qui va leur servir à chiffrer leurs communications. La création et l'échange de cette clé est un mécanisme relativement lourd et long à mettre en oeuvre. 802.11i propose une mise en cache de ces clés. Ainsi, une station déconnectée qui retourne sur le réseau sera immédiatement associée, la clé étant restée en cache.

Un autre mécanisme particulièrement intéressant consiste pour une station à pouvoir se préauthentifier. Pendant qu'une station émet sur un AP, elle peut s'authentifier aupès d'un deuxième AP et générer à l'avance les clés de chiffrement.

Comme nous l'avons vu lors du chapitre sur 802.11F, la cause majeure du point de lenteur provient du temps mis par une station à s'authentifier. Avec 802.11i, ce temps peut être réduit à zéro. En effet, soit la station a déjà été authentifiée et la clé est réutilisée, soit la station continue à communiquer avec l'ancien AP pendant que la transaction d'authentification s'effectue avec le nouvel AP. Dans ce contexte, la bascule devient plus rapide.

2. Les solutions propriétaires

Du fait de l'inefficacité de 802.11F, de la montée en puissance de la VoIP et de l'interêt commercial suscité par une solution non interopérable, les constructeurs déployent leurs propres solutions permettant le roaming en wifi.

Ces solutions écartent certaines contraintes initiales posées par 802.11F. Une illustration marquante de cette démarche consiste à utiliser un point central qui va diriger les actions des AP, au contraire d'IAPP qui est décentralisé. Les constructeurs peuvent se permettre cette utilisation car ils ont la main sur l'architecture wifi, l'ensemble des AP et le DS.

Par exemple, Cisco propose depuis longtemps des réseaux wifi qui permettent à des téléphones wifi de roamer. Il s'agit bien évidemment d'une technologie non documentée publiquement.

Le protocole employé s'appelle LWAPP pour LightWeight Access Point Protocol. C'est un réseau Wifi basé autour d'un point central. Cisco parle d'intelligence centralisée. Les points d'accès sont des points d'accès légers. Nous pouvons supposer que le fait d'avoir un point central facilite la gestion du roaming. De plus, un paramétrage spécial doit être activé sur le point central pour autoriser le roaming de la VoIP. Enfin ce point central constitue l'unique sortie de tous les postes Wifi vers l'extérieur.

De la même manière tous les constructeurs qui vendent des solutions complètes de wifi incluant le roaming proposent des points centraux et des AP légers à déployer géographiquement. Le point central d'ailleurs n'a généralement pas d'antenne wifi. Il n'est présent que pour piloter les AP et lier le système de distribution à un autre réseau, comme le LAN d'entreprise.

En conclusion, les constructeurs ont réutilisé les solutions efficaces des réseaux GSM, c'est à dire un fonctionnement par cellule, avec un point central fédérant de multiples AP. Actuellement, il n'existe que des réseaux avec une seule cellule, mais rien ne permet d'empêcher de penser à des réseaux dotés de multiples cellules dans un avenir proche.

3. Un comparatif de quatres solutions

En janvier 2007, le laboratoire "groupe tests" a testé plusieurs solutions de mise en réseau wifi. Ce laboratoire réalise toutes les mesures de grandeurs techniques informatiques pour les journaux comme 01 réseau, décisions informatiques, etc..

Le test portait sur plusieurs points comme la sécurité, la facilité de gestion, la détection d'intrusions, mais également le point étudié ici qui correespond au temps mis par une station pour roamer d'un AP à un autre. Seule cette mesure est reprise ici.

La méthode employée pour faire roamer une station a été de prendre un ordinateur portable et de se déplacer à pied d'un AP vers un autre.

Les quatre solutions choisies fonctionnent toutes avec un point central et des AP légers.

Blue Socket: Central BSC 400 et AP BSAP 1500. Le temps de bascule est de 235.5 ms.

Aruba Networks: Central Aruba 800 et AP AP65. Le temps de bascule est de 128.9 ms.

Colubris networks: Central MSC-5100 et AP MAP330. Le temps de bascule est de 610 ms.

Trapeze Networks: Central MX-8 Mobility et AP MP372. Echec de la bascule.

Ces tests montrent que la durée prise par le roaming est encore trop grande pour faire de la VoIP (rappel: il faut moins de 50ms) y compris avec ces solutions intégrées. Mais ces valeurs peuvent s'expliquer par le fait d'une part que le test ne visait pas explicitement le roaming mais plutot la sécurité. D'autre part, certains boîtiers ont des paramétrages spécifiques "VoIP" à mettre en oeuvre pour faire de la téléphonie. Notamment le boîtier Aruba qui ne propose la VoIP en wifi qu'à partir de la version 3 de son système. L'échec de la bascule pour Trapeze Networks est dû à un bug dans le serveur DHCP qui doit être corrigé à l'heure actuelle.

Il n'a pas été possible de trouver de la documentation technique sur aucun des mécanismes mis en jeu par ces constructeurs pour effectuer le roaming. Les plaquettes commerciales sont la seule source d'information sur les performances et la fiabilité du roaming.

Ainsi, le roaming en wifi est une réalité aujourd'hui, poussée par le développement de la VoIP. C'est un technologie encore jeune, en constante évolution.

4. Conclusion

Le roaming en wifi, bientôt dépassé et complété par le roaming multi technologies?

1. L'obligation de choisir un constructeur pour roamer

Comme nous l'avons vu, il n'existe pas encore de norme ouverte qui permette de roamer en wifi. Toute entreprise désirant mettre en place une infrastructure wifi qui lui permette en plus de roamer (avec une pensée toute particulière vers la VoIP) doit faire le choix d'un constructeur.

Il n'existe aucune norme d'interopérabilité entre les différents constructeurs.

2. Vers la convergence wifi / GSM?

Dès que la question de la téléphonie over Wifi est levée, se pose immanquablement la question de l'interopérabilité avec le réseau GSM. Ce champ d'application sort du cadre de cet exposé, mais il faut savoir que des constructeurs vendent déjà des téléphones disposant d'une antenne wifi et d'une antenne GSM.

Le côté pratique est immédiat. Les personnes disposent d'un matériel unique, avec un numéro unique. Un deuxième point concerne l'aspect financier puisque tous les appels utilisant le réseau Wi-Fi sont gratuits.

De ce fait, l'IEEE travaille déjà sur la future norme 802.21 qui permettra une convergence totale réseau GSM, réseau Wi-Fi et réseau bluetooth.

Cette norme 802.21 devrait permettre le choix du réseau (bluetooth, wifi, GSM) et le roaming de manière optimale. Cette norme est en cours d'étude par l'IEEE.

Références:

[1] Norme 802.11
-La norme
http://grouper.ieee.org/groups/802/11/main.html
-Le schéma complet du protocole
http://www.oreillynet.com/wireless/2005/05/20/graphics/802.11Poster.pdf

[2] Cours sur le WiFi
http://www.urec.cnrs.fr/IMG/pdf/Cours.06.sansfil.2-theorie.pdf

[3] Roaming et interoperabilité. Article écrit en 2004.
http://www.techworld.com/features/index.cfm?featureID=1023&printerfriendly=1

[4] Norme 802.11F
http://standards.ieee.org/getieee802/download/802.11F-2003.pdf
-Notification de l'abandon de la norme sur le calendrier 802.11:
http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

[5] Norme 802.11k
Actualité du projet:
http://grouper.ieee.org/groups/802/11/Reports/tgk_update.htm

[6] Norme 802.11r
Actualité du projet:
http://grouper.ieee.org/groups/802/11/Reports/tgr_update.htm

[7] Norme 802.11i
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[8] Editeur futsoft. Vente d'une pile 802.11F portable.
-Page du site web concernant 802.11F
http://www.futsoft.com/802_11F.htm
-Spécifications technique. Lien trouvé par google, mais lien cassé:

```
802.11F (IAPP)
Format de fichier: PDF/Adobe Acrobat
implementation of the 802.11F specification for ... incorporate the 802.11F
IAPP functionality into their WLAN products. ...
www.futsoft.com/pdf/802.11Ffs.pdf
```

[9] hostpad (linux)
http://hostap.epitest.fi/hostapd/
-Fichier iapp.c:
http://www.google.com/codesearch?hl=en&q=+iapp.c+hostapd+show:Gm4dLaWsT5M:kNcEXU3sFdA:mpFZ8Kan86A&sa=N&cd=3&ct=rc&cs_p=http://hostap.epitest.fi/releases/snapshots/hostapd-0.6-2007-02-11.tar.gz&cs_f=hostapd-0.6-2007-02-11/iapp.c#a0
-mailing list:

http://lists.shmoo.com/pipermail/hostap/

[10] hostpad (openBSD)
La manpage d'hostpad, et d'hostapd.conf:
http://www.openbsd.org/cgi-bin/man.cgi?query=hostapd
http://www.openbsd.org/cgi-bin/man.cgi?query=hostapd.conf

[11] VoIP
http://en.wikipedia.org/wiki/VoIP

[12] Méthodes de mesure et mesures du roaming en wifi
http://www.winmee.org/2005/papers/WiNMee_Gonzalez.pdf
http://portal.acm.org/ft_gateway.cfm?id=1023788&type=pdf&coll=&dl=ACM&CFID=15151515&CFTOKEN=6184618
http://lion.cs.uiuc.edu/group_seminar_slides/WLANhandoff-042705.pdf
http://www.cs.wisc.edu/~arunesh/thesis.pdf
http://rio.ecs.umass.edu/mnilpub/papers/Yliao-handoff-tech.pdf

[13] Magazines
Contrôleurs wifi:
-Décision Informatique. Numéro 701 du 8 au 14 janvier 2007.
-01 Réseaux. Numéro 168 / Janvier 2007.
Convergence wifi / GSM
-Décision Informatique. Numéro 711 du 19 au 25 mars 2007.

[14] Faiblesses du WEP, attaque de Fluhrer, Mantin et Shamir.

http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf