

**Livrable L2.1: Étude de de la signalisation standardisée pour l’Association Client-Point d’Accès et Point d’Accès-Contrôleur**

Partenaires impliqués: CTP, L2S, COMSIS

**Auteurs:** Mohamed Amine KAFI

Alexandre Mouradian

Véronique Vèque

Table des matières

[1Introduction 5](#__RefHeading___Toc3275_173870930)

[2Association des clients aux points d’accès 6](#__RefHeading___Toc3277_173870930)

[2.1Association basée sur le standard 802.11 6](#__RefHeading___Toc3279_173870930)

[2.1.1Balayage passif (Passive Scan) 6](#__RefHeading___Toc3281_173870930)

[2.1.2Balayage actif (Active Scan) 6](#__RefHeading___Toc3283_173870930)

[2.2Les problèmes associés à 802.11 6](#__RefHeading___Toc4063_459909576)

[2.3Association basée sur l’optimisation de paramètres 7](#__RefHeading___Toc3285_173870930)

[3Les approches d’association centralisées et distribuées 8](#__RefHeading___Toc3287_173870930)

[3.1Introduction 8](#__RefHeading___Toc2659_891654353)

[3.2Optimisation globale du débit sans équité entre clients 10](#__RefHeading___Toc3291_173870930)

[3.3Optimisation du débit avec équité 11](#__RefHeading___Toc3293_173870930)

[3.3.1Sans considérer les AP 11](#__RefHeading___Toc3295_173870930)

[3.3.2Équité basée sur le temps attribué 11](#__RefHeading___Toc3297_173870930)

[3.3.3Équité basée sur le débit ou l’accès 12](#__RefHeading___Toc3299_173870930)

[3.4La réassociation des stations avec les AP 13](#__RefHeading___Toc3303_173870930)

[3.5Les approches distribuées 14](#__RefHeading___Toc3305_173870930)

[4Signalisation lors de l’association des clients aux points d’accès 14](#__RefHeading___Toc3317_173870930)

[4.1Le balayage 15](#__RefHeading___Toc3319_173870930)

[4.2Authentification 15](#__RefHeading___Toc3321_173870930)

[4.3Association 15](#__RefHeading___Toc3323_173870930)

[5Signalisation Permettant la communication entre les points d’accès et le contrôleur (CAPWAP) 15](#__RefHeading___Toc3325_173870930)

[5.1Objectifs du protocole CAPWAP 15](#__RefHeading___Toc3327_173870930)

[5.2Différentes architectures réseaux possibles 16](#__RefHeading___Toc3329_173870930)

[5.3Architectures MAC prises en charge par le protocole CAPWAP 17](#__RefHeading___Toc3331_173870930)

[5.3.1Architecture MAC locale (Local MAC) 17](#__RefHeading___Toc3333_173870930)

[5.3.2Architecture MAC fractionnée (Split MAC) 18](#__RefHeading___Toc3335_173870930)

[5.3.3Architecture MAC distante (Remote MAC) 18](#__RefHeading___Toc3337_173870930)

[5.4Interface de communication entre WTP et AC 18](#__RefHeading___Toc3339_173870930)

[5.5Les liaisons avec 802.11 20](#__RefHeading___Toc3345_173870930)

[5.5.1LOCAL MAC 21](#__RefHeading___Toc3347_173870930)

[5.5.2SPLIT MAC 22](#__RefHeading___Toc3349_173870930)

[5.5.3La procédure de changement de WTP (Roaming) 23](#__RefHeading___Toc3351_173870930)

[6Changement de point d’accès transparent aux clients (Roaming déclenché par l’AP) 23](#__RefHeading___Toc4065_459909576)

[7Quelques travaux des groupes IEEE 802.11 et leurs améliorations 24](#__RefHeading___Toc4067_459909576)

[7.1802.11e,MAC amélioration concernant la qualité de service (QoS) 25](#__RefHeading___Toc3309_173870930)

[7.2802.11k, radio resource measurement 26](#__RefHeading___Toc3311_173870930)

[7.3802.11r, fast basic service set transition 27](#__RefHeading___Toc3313_173870930)

[7.4802.11v, Wireless network management: 27](#__RefHeading___Toc3315_173870930)

[8Bilan 27](#__RefHeading___Toc3357_173870930)

[A1 Interface de communication entre WTP et AC selon le protocole CAPWAP 29](#__RefHeading___Toc1542_1347476463)

[A2 Les liaisons du protocole CAPWAP avec 802.11 30](#__RefHeading___Toc4069_459909576)

[A3 Différentes informations radio couvertes par l’amendement 802.11k 31](#__RefHeading___Toc1773_1706799328)

[A3.1 Informations sous forme de demande/ réponse 31](#__RefHeading___Toc1775_1706799328)

[A3.2 Informations sous forme de demande seule (sans rapport) 31](#__RefHeading___Toc2861_1297181907)

[A3.3 Informations sous forme de rapport seul (sans demande) 31](#__RefHeading___Toc2863_1297181907)

[A4 Différents services et mécanismes offert par l’amendement 802.11v 32](#__RefHeading___Toc1777_1706799328)

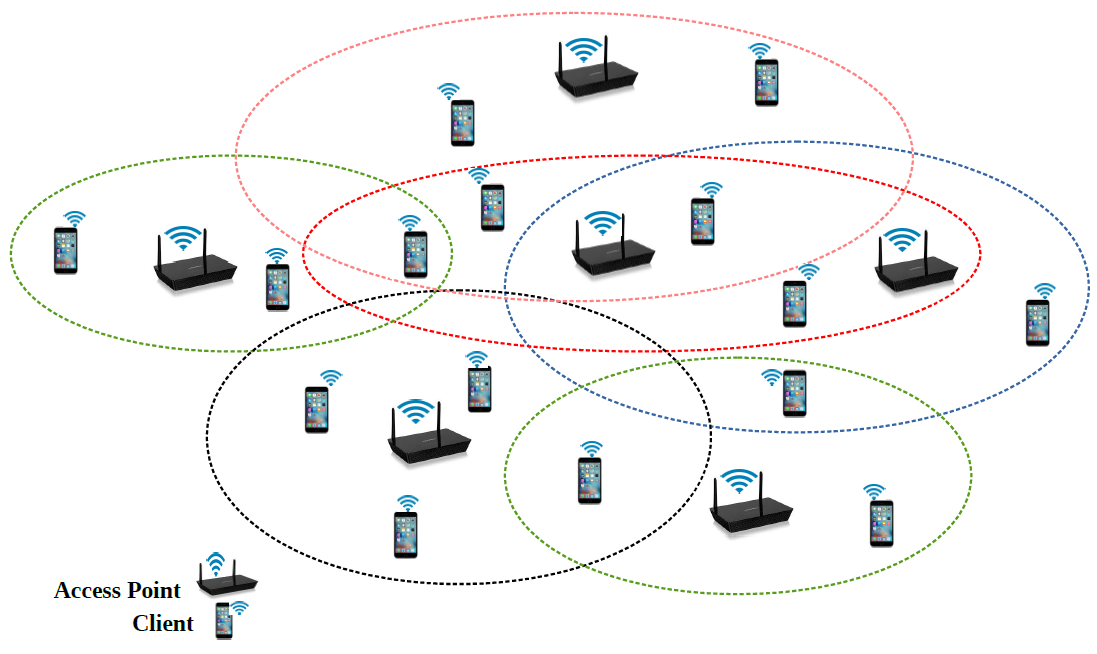
[Glossaire 34](#__RefHeading___Toc4071_459909576)

[Références bibliographiques 36](#__RefHeading___Toc4073_459909576)

# Introduction

La multiplication des terminaux sans fil comme les tablettes et les smart phones ainsi qu’une offre importante d’applications ont conduit à un déploiement de plus en plus dense des réseaux sans fil utilisant la technologie Wi-Fi. Dans un tel environnement, les points d'accès (ou AP, Access Point) sont très proches les uns des autres et leur couverture radio se chevauche mutuellement. Des exemples de réseaux Wi-Fi denses sont les réseaux des particuliers où chaque appartement possède sa propre box qui fait aussi AP et les réseaux d’entreprise qui sont couverts par de multiples AP à chaque étage ou couloir.

Dans une entreprise, le WLAN (Wireless Local Network) constitue un réseau multi-cellulaires tel que montré sur la Figure 1. L’avantage d’une telle configuration est une meilleure couverture de tous les usagers. Cependant, le nombre de canaux orthogonaux étant limité, leur réutilisation est élevée et les cellules proches interfèrent beaucoup entre elles augmentant le taux de collisions et réduisant le débit utile. A l’heure actuelle, l’association des terminaux à un AP se base sur la plus forte puissance de signal reçue ce qui peut conduire à un déséquilibre dans la charge des AP. Certains AP chargés ne peuvent ainsi satisfaire les besoins des utilisateurs en débit et qualité de service (QoS- quality of service).



**Figure1: Réseau Wi-Fi dense composée de cellules se chevauchant**

L’objectif de ce rapport est de faire le point sur l’optimisation d’utilisation des ressources radio dans les réseaux locaux sans fil. Le paragraphe 2 décrit l’association des clients avec les AP selon le standard et les méthodes optimisées. Le paragraphe 3 détaille les méthodes d’association basées sur l’optimisation de paramètres. Le paragraphe 4 présente la signalisation utilisée lors de l’association d’un client avec l’AP utilisant la norme 802.11. Ensuite, le paragraphe 5 décrit le protocole de signalisation CAPWAP qui gère la relation Point d’Accès-Contrôleur Central. Le paragraphe suivant présente le protocole ODIN qui vise à gérer le changement des Point d’Accès d’une manière transparente pour le client. Différents amendements du protocole 802.11 qui visent à améliorer la gestion des ressources radio sont décrits dans le paragraphe 7. On terminera le document par le paragraphe 8 qui décrit les axes méritant d’être améliorés pour une gestion optimale des ressources radio dans un WLAN.

# Association des clients aux points d’accès

L’association d’un terminal à un point d’accès est l’opération de connexion effective au point d’accès qui suit l’authentification du terminal.

## Association basée sur le standard 802.11

Dans le standard IEEE 802.11 [1], l’association d’un terminal se fait en fonction de la puissance du signal reçu RSSI (Received Signal Strength Indicator) des AP. A chaque fois qu’une nouvelle station rejoint le réseau, elle effectue une opération de balayage des canaux passif ou actif pour découvrir les points d'accès disponibles dans le voisinage. La station choisit de s’associer à l’AP qui présente le RSSI le plus fort.

### Balayage passif (Passive Scan)

Chaque point d'accès envoie périodiquement une trame de balise ou *beacon* qui contient des informations de synchronisation, son identité (BSSID et SSID), la liste des débits supportés par l’AP, la méthode de sécurité utilisée [25]. La station qui arrive parcourt tous les canaux disponibles et analyse les *beacons* reçus des AP voisins sur chaque canal. Elle décide de s’associer avec l’AP ayant émis avec le plus fort RSSI. Après avoir choisi le point d'accès, un processus d'authentification doit être effectué par l’échange d’une preuve entre la paire station–point d’accès. Une fois l’association effective, l’AP enregistre l’adresse MAC de la station (point de raccordement) et les mécanismes réseau assurent la connectivité de niveau supérieur (distribution d’une adresse IP).

### Balayage actif (Active Scan)

Dans ce cas, la station scanne les canaux disponibles et, à chaque fois, elle n'attend pas la réception des balises (beacons) des AP disponibles, mais demande elle-même à ces points d'accès via des trames de sonde (probe request frame), pour lesquels les points d'accès répondent par des trames de réponse de sonde (probe response frame). L’association est la même qu’en balayage passif.

## Les problèmes associés à 802.11

La capacité du lien entre un client et un AP dépend de l’atténuation du signal (pertes en espace libre et fading), du bruit et des interférences. L’atténuation limite le débit physique et les interférences augmentent le taux d’erreurs.

Cela conduit à utiliser différents systèmes de modulation et codage (SMC). En effet, avec un taux d’erreurs élevés, on choisira une modulation simple et une redondance importante qui entraînent un débit plus lent. Par conséquent, chaque client obtient un débit différent selon sa position et son environnement. Le réseau est alors multi-débits.

Un autre problème provient de la méthode d’accès DCF utilisée par défaut pour ordonnancer les communications des stations appartenant au même AP. DCF garantit que chaque client aura la même probabilité de transmission c’est-à-dire que chaque client peut transmettre une trame de taille maximale avec la même probabilité mais chacun à un débit différent.

Cela conduit sur le long terme à ce que toutes les stations transmettent au même débit sur la voie montante qui est celui de la station la plus lente (ceci est connu sous le nom de l’anomalie 802.11 [3-5,9]).

## Association basée sur l’optimisation de paramètres

La stratégie d’association standard que nous venons de voir, n'est pas la meilleure dans un environnement de réseaux WLAN multi-cellulaires car elle ne tient pas compte de la **charge** des AP. Mieux choisir le point d’accès auquel s’associer présente de nombreux avantages tels qu’équilibrer la charge entre les AP, réduire les interférences entre les points d’accès proches, ou mieux satisfaire les besoins des clients en termes de débit ou de QoS. Choisir le meilleur point d’accès auquel associer un client peut être effectué de manière centralisée ou distribuée. Dans le cas centralisé, un contrôleur a une vue globale de tout le réseau et de l’utilisation des ressources, à travers les informations envoyées par les points d’accès placés sous sa responsabilité ainsi qu'éventuellement d'autres informations provenant des clients eux-mêmes. La deuxième option consiste à effectuer l'association par une décision distribuée prise par le client lui-même ou par les points d’accès à proximité, sans passer par un contrôleur central. Les approches centralisées nécessitent plus de communications et de collaboration au sein du réseau, mais elles donnent une vision globale des ressources qui permet un débit agrégé plus haut et une meilleure équité [2]. Cependant, en fonction de la taille du réseau et de la difficulté de gestion des paramètres qui en résulte, cette approche n’est pas toujours efficace, ce qui pousse vers l'utilisation de stratégies d'association distribuées au niveau des clients eux-mêmes [27] ou des points d'accès individuellement [28]. Dans ce cas, le volume de signalisation est inférieur à celui de l’approche centralisée, mais l’utilisation des ressources ne sera pas optimale du fait d’une perception seulement locale de l’état du réseau [2]. La Figure 2 ci-dessous, résume ces approches.

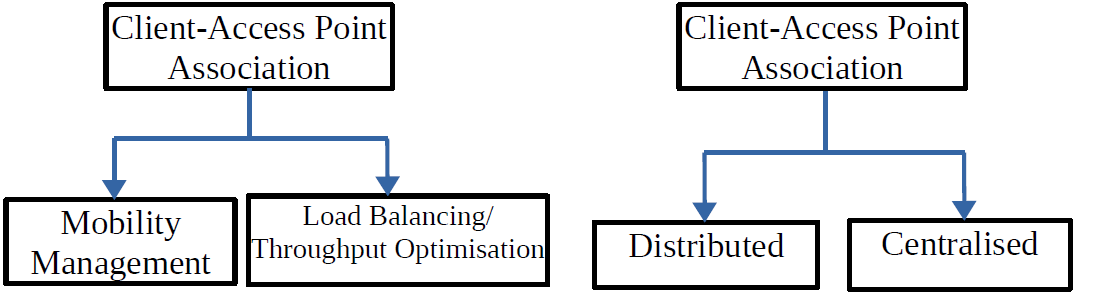


Figure 2: Types d’associations des clients aux points d’accès

Que la sélection du point d'accès soit centralisée ou distribuée, plusieurs métriques peuvent être maximisées [2] telles que le débit global [8-10], le débit individuel [31-32], le taux de livraison de paquets [27], l’équité en charge [34] ou la conservation de l’énergie [29].

La littérature porte majoritairement sur l’optimisation centralisée du débit global qui vise à utiliser le mieux possible les AP et les ressources de transmission tout en tenant compte des besoins relatifs de chaque client; on parle d’équité proportionnelle ou relative. Les stratégies distribuées basées sur les AP peuvent aussi assurer cette équité entre leurs clients.

Dans l'association standard, la mobilité du terminal change la puissance du signal avec l’AP et déclenche une réassociation aussi appelée itinérance (roaming). De même, si les paramètres d’un client déjà associé changent, on peut déclencher une réassociation avec un autre point d'accès. Faire cette réassociation de manière transparente, sans perte de paquets de données ni délai élevé, revêt une grande importance pour la qualité des applications.

La réalisation de ces nouvelles techniques d’association différentes de la norme IEEE802.11 a un impact sur le logiciel, pour le point d'accès et/ ou pour le client. En association centralisée, il est possible de ne faire des modifications qu'au niveau AP, si le client ne doit pas communiquer d'informations supplémentaires à celles spécifiées par la norme. Si le client doit communiquer des informations de signalisation (comme l’interférence de son voisinage), alors il sera également nécessaire de modifier le logiciel au niveau du client. C’est le cas, par exemple, pour l'association distribuée, décidée par le client.

La Figure 2 montre deux axes de classification de l'association client-AP. Selon le premier axe à gauche, l’approche se fait selon la mobilité du client ou à travers des critères d’optimisation. Le deuxième axe adresse la gestion distribuée versus centralisée.

# Les approches d’association centralisées et distribuées

## Introduction

Dans les approches centralisées, la prise de décision s’effectue au niveau d’un contrôleur unique localisé dans une machine du réseau. Ce contrôleur peut être localisé dans un AP particulier, un serveur de gestion [3], ou un routeur. Si le réseau est très étendu, un contrôle hiérarchique peut être effectué par différents niveaux de contrôleurs gérant chacun un ou plusieurs sous-réseaux.

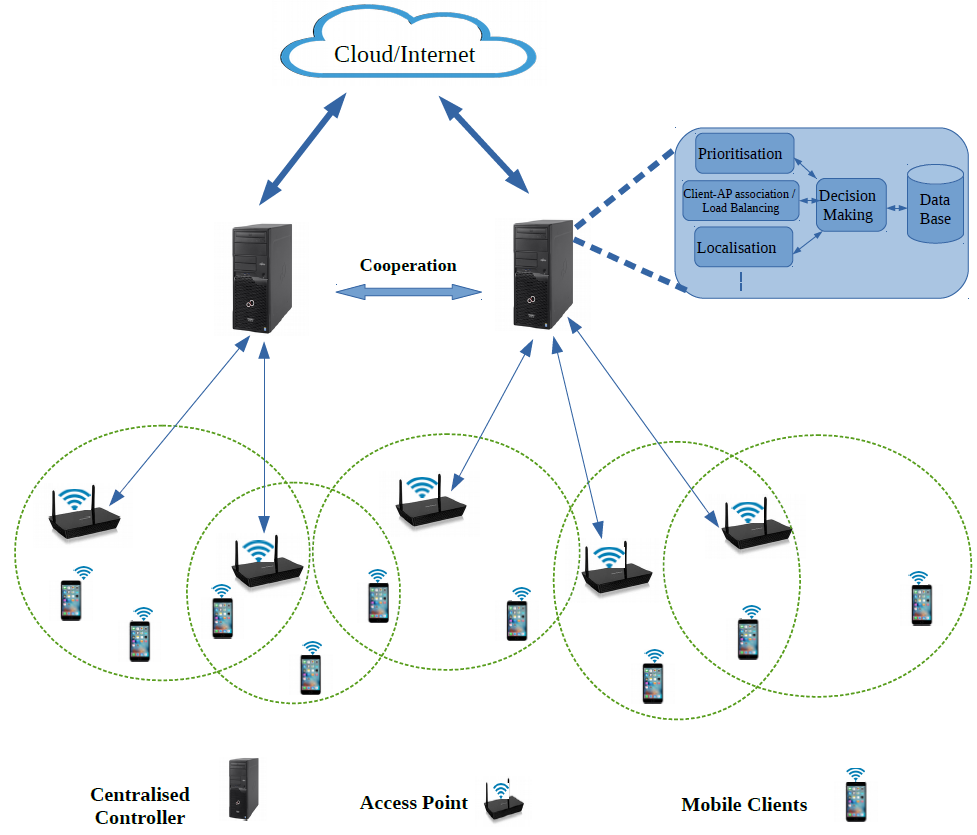


Figure 3: Architecture d’un réseau WLAN multi-cellules avec un contrôleur centralisé [2].

Les tâches du contrôleur ne sont pas seulement l'association client-point d'accès, mais également la sélection de canaux, le contrôle de niveau de puissance d’émission des AP ou des stations [29] et l’ordonnancement des communications [33].

Dans le cadre de l'approche de programmation des fonctionnalités des contrôleurs réseau, d'autres tâches pourraient être envisagées à l'avenir selon les exigences requises par les applications, comme la QoS, plusieurs niveaux de fiabilité, la prise en compte des contraintes en temps-réel, etc. [2,25]. Si l’on étend la coordination entre des contrôleurs d’opérateurs différents, on peut améliorer encore la performance du réseau hors association. En effet, si par exemple deux opérateurs offrent l’accès dans un même endroit (centre commercial, ville…) leur coopération permettrait une meilleure gestion des interférences même si leurs abonnés n’utilisent pas le même réseau [30]. La Figure 3 ci-dessus illustre une telle architecture.

Dans un réseau WLAN multi-cellules, la méthode standard d’association ne prend pas en compte la différence de débit obtenu par le client selon l’AP auquel il est associé (cf. partie 2.2). Ce qui est un inconvénient majeur. Un contrôleur qui connaît toutes les capacités des liens entre un client et tous les AP peut optimiser le débit offert au client en choisissant la meilleure association (meilleure selon le critère optimisé).

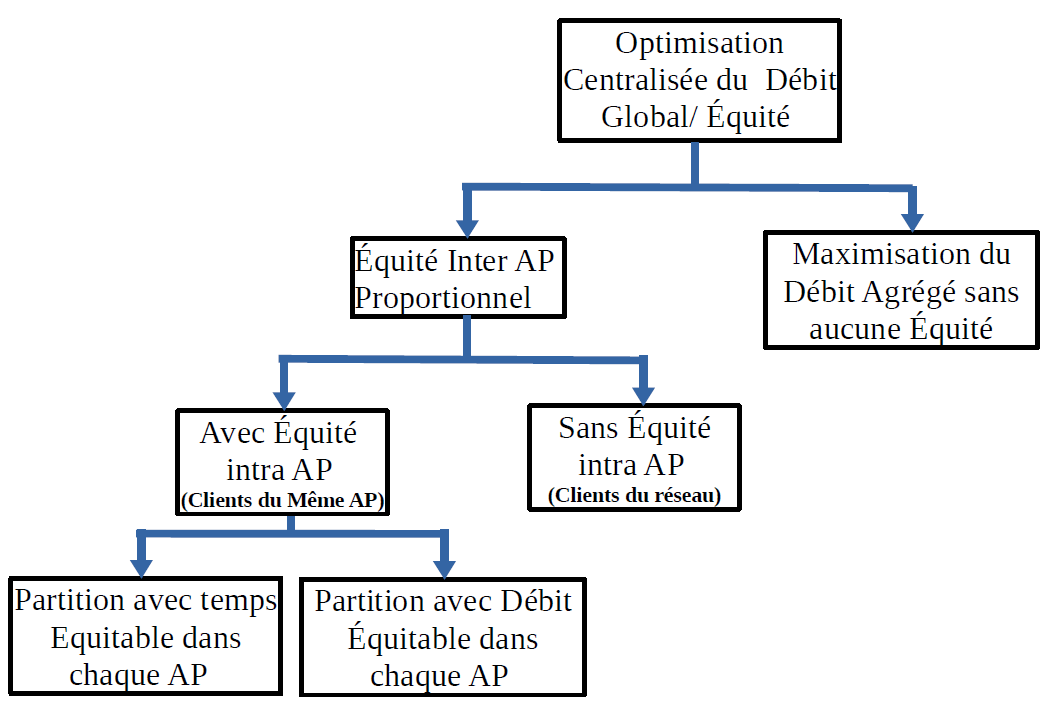


Figure 4 : Classification des méthodes d’association centralisée des clients avec les AP.

Les méthodes centralisées d’association optimisée visent à maximiser le débit agrégé du réseau et permettent de corriger en partie ces défauts. Le résultat de l’optimisation est l’affectation d’un client à un AP avec un débit imposé. Plusieurs méthodes centralisées existent. Leurs différences résident dans la façon dont elles assurent l’équité entre les clients. L’objectif étant de maintenir un équilibre entre la maximisation du débit global et l’allocation d’un débit minimal à chaque client, relativement à son besoin. La Figure 4 montre une classification des méthodes qui optimisent le débit global du réseau. On distingue d’abord les méthodes qui assurent l’équité entre clients de celles qui ne le font pas [7]. Parmi les méthodes avec équité, on distingue ensuite celles qui considèrent tous les clients du réseau [3] de celles qui traitent AP par AP [10]. Dans cette dernière classe, l’allocation des ressources est assurée en temps attribué (time fairness) ou bien en débit au sein d’une même AP (access fairness).

## Optimisation globale du débit sans équité entre clients

Dans ce type d’optimisation d’association, l’objectif est d’augmenter le débit global du réseau [7], sans prendre en compte aucune équité entre les débits offerts aux stations du réseau. En effet, le débit global est obtenu par la somme des débits des clients connectés aux différentes AP. Par conséquent, les stations ayant un lien de débit élevé monopolisent les communications et celles ayant des liens de débits faibles se trouvent lésées.

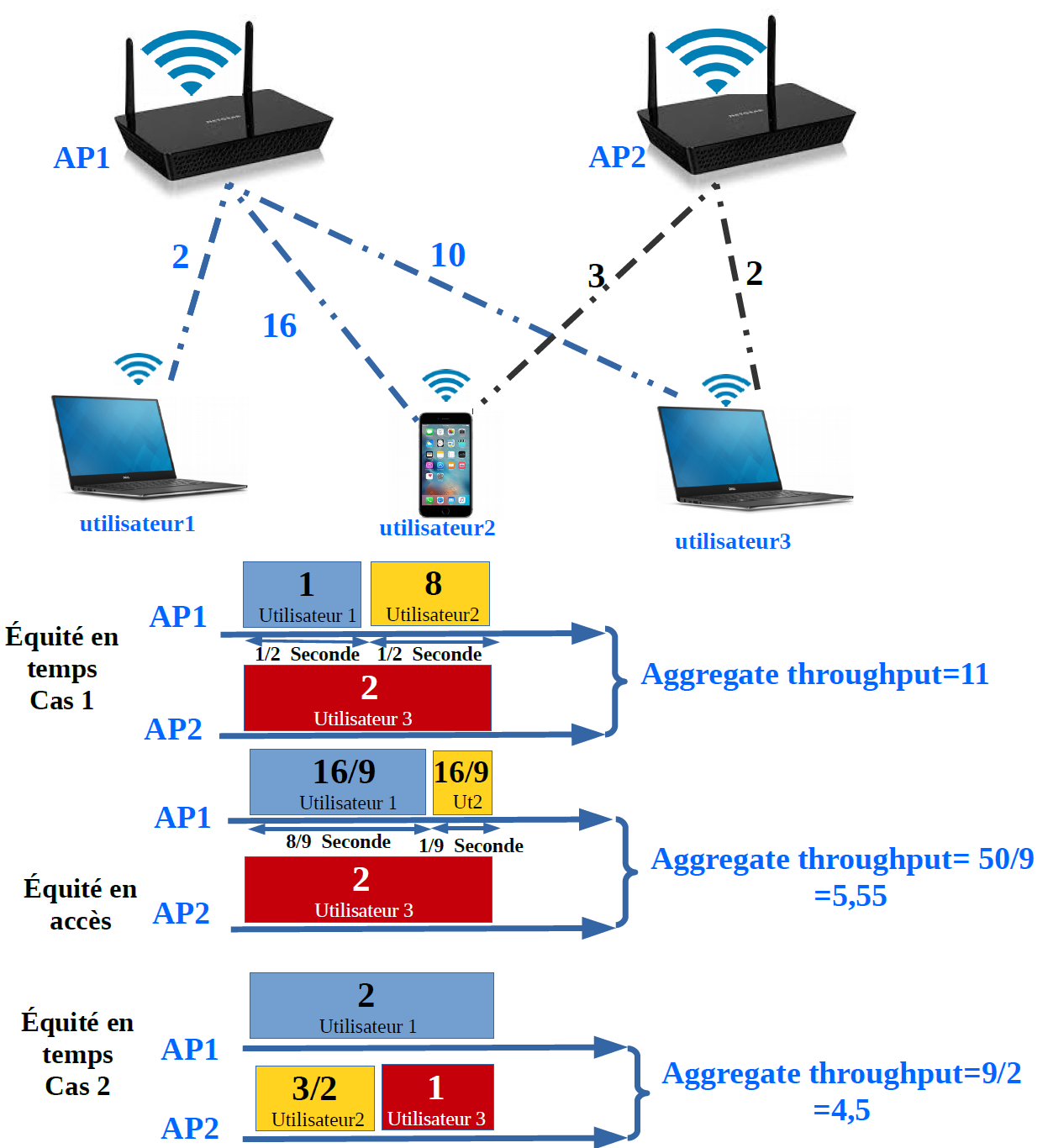


Figure 5 : Associations de clients aux AP selon l’équité en temps et l’équité en accès.

Dans la Figure 5, on considère 2 AP et 3 terminaux. Les terminaux peuvent obtenir un débit maximal (valeur associée à chaque lien) en se connectant seuls à l’un des deux AP. En maximisant le débit global du réseau, l’utilisateur 2 sera associé à l’AP1 et l’utilisateur 3 à l’AP2, ce qui va donner un débit agrégé du réseau égal à 18, mais qui bien-sûr n’attribue aucune ressource à l’utilisateur 1.

## Optimisation du débit avec équité

L’équité proportionnelle est assurée en introduisant la fonction logarithmique dans la fonction *objectif global* qui sera optimisée par le contrôleur central. Cette fonction est décrite en détails dans [6]. En fait, la présence de la fonction «logarithmique» dans la fonction *objectif* de maximisation du débit favorise une proportionnalité entre les valeurs faible et haute, car la présence de nombreuses valeurs faibles ayant une valeur de fonction logarithmique petite ou négative diminue la somme dans la fonction objectif, ce qui favorise un équilibre entre ces valeurs et les valeurs élevées dans la fonction objectif globale.

La fonction utilitaire à optimiser pour chaque utilisateur j est:

Uj=∑**i**∈**A** x**ij** . bij.

avec A l’ensemble des AP présents dans le réseau et U est l’ensemble des utilisateurs du réseau qui sont concernés par l’optimisation. La variable x**ij** est une variable binaire prenant les valeurs 0 ou 1 pour mentionner que l’utilisateur Uj est bien associé à l’APi si la valeur est égale à 1, ou bien qu’il n’est pas associé si la valeur est égale à 0. La valeur bij est le débit que peut obtenir l’utilisateur Uj quant il est associé à l’APj. Ce débit dépend de la qualité du lien avec l’AP (le SINR - Signal over Interference plus Noise Ratio) et du nombre de clients associés à l’AP.

Le problème d’optimisation prend alors la forme suivante:

**Max** ∑ **j**∈**U** log (∑**i**∈**A**  x**ij** . bij)

**Tels que:**

bij= xij .tij .rij  ∀ i ∈ A, ∀ j ∈ U.

∑ i∈A xij =1 ∀ j ∈ U ,

xij ∈ {0,1} ∀ i ∈ A, ∀ j ∈ U,

0 ≤ tij ≤ 1 ∀ i ∈ A, ∀ j ∈ U.

∑ j∈U tij ≤1 ∀ i ∈ A ,

### Sans considérer les AP

L’optimisation du débit agrégé du réseau est faite entre tous les clients du réseau quelques soient les points d’accès. On parle d’équité proportionnelle globale, aucune équité n’étant réalisée entre les clients d’un même AP ni en accès ni en temps.

On résout alors directement le problème d’optimisation énoncé ci-dessus.

### Équité basée sur le temps attribué

On a vu que certains travaux imposent une forme d’équité au sein de chaque AP pour les clients qui y sont connectés. Nous nous focaliserons sur la voie descendante qui est dominante dans les réseaux WiFi [10].

Une première forme d’équité consiste à allouer une durée de communication égale pour les clients d’un même AP. C’est l’approche suivie dans [3]. Dans ce cas, le débit bij qu’obtient un client j dans l’APi dépend de rij et de la proportion de temps qui lui est alloué (nombre de clients de l’AP):

bij= et aussi tij=

Comme on alloue une proportion de temps égale à chaque station cliente cette proportion est égale à l’inverse du nombre de clients associés à cette AP. On note que les débits obtenus sont différents pour chaque client car ils reçoivent (ou émettent) à des débits différents durant la période de temps équitable qui leur est allouée. Leur débit dépendent de la qualité du lien avec l’AP comme illustré dans la Figure 6 pour un AP et deux clients. Le problème d’optimisation est resolu avec la prise en consideration de la contrainte precedante.

La Figure 5 montre des exemples de débits obtenus pour plusieurs associations avec l’équité en temps au niveau de l’AP. En effet, dans l’exemple d’équité en temps cas 1, l’association des clients 1 et 2 à l’AP1 et le client 3 à l’AP2 permet d’avoir un débit agrégé de 11 qui est plus optimal que l’association des clients 1 à l’AP1 et 2 et 3 à l’AP2, qui est mentré dans l’exemple d’équité en temps cas 2, puisque elle offre un débit arégé de 4,5. Cela montre l’interet de l’optimisation centralisée d’association.

Il est à noter que la mise en œuvre de ce type d’équité au sein de l’AP semble difficile. En effet, au niveau de la voie descendante (dowlink), il faudrait modifier l’ordonnancement des transmissions dans l’AP pour respecter les proportions de temps en fonction des débits de chaque utilisateur ce qui n’est pas trivial dans un réseau avec des tailles de paquets et des taux d’arrivées différents. Pour la voie montante (uplink), il faudrait changer de méthode d’accès (DCF ne permet pas une équité en temps, mais en accès comme évoqué précédemment).

### Équité basée sur le débit ou l’accès

Un deuxième type d’équité consiste à donner le même débit bij à chaque client. Dans ce cas, le temps d’occupation du canal est alors différent pour chaque client et dépend de rij comme illustré sur la partie droite de la Figure 6 et dans la Figure 5. Ainsi, les clients les plus lents occupent le support pendant une période plus longue que les clients rapides pour l'envoi du même volume de données [3]. C’est l’approche adoptée dans [10].

Dans ce cas on résout toujours le même problème d’optimisation, mais avec la contrainte supplémentaire:

bij=

Ce type d’équité est plus facile à mettre en œuvre au niveau de l’AP sur la voie descendante: avec un ordonnancement Fair Queuing de la file d’attente de transmission par exemple. Sur la voie montante, c’est ce type d’équité qui est obtenu avec DCF.

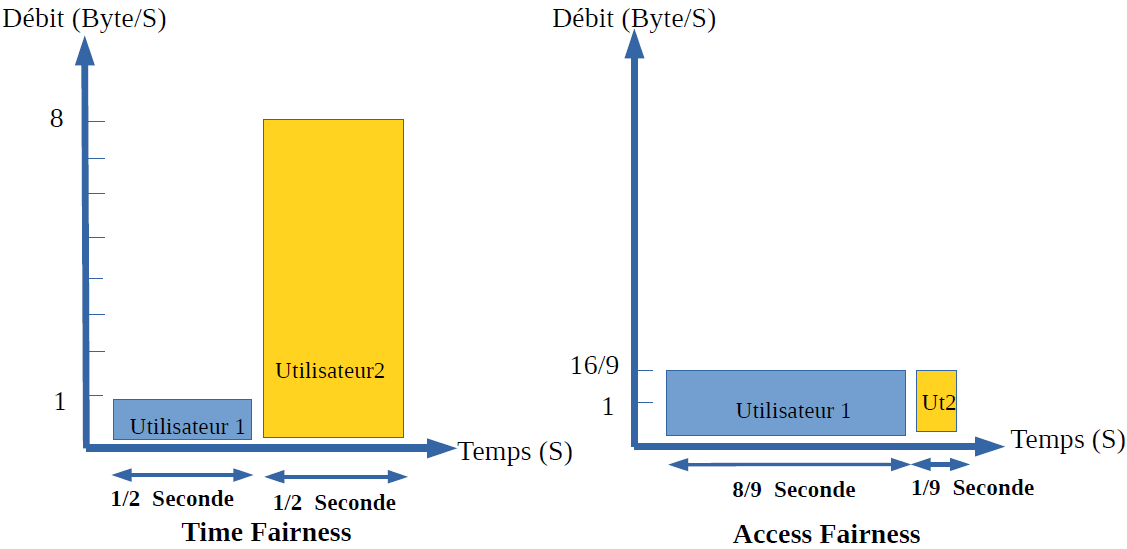


Figure 6: La différence de débits entre l’équité en temps et en accès

## La réassociation des stations avec les AP

Si les clients sont présents à l’initialisation du réseau, une optimisation hors connexion (offline) des associations peut être effectuée. En réalité, les clients arrivent au fil de l’eau, ce qui nécessite une association incrémentale (en ligne). Résoudre le problème d’optimisation global à chaque arrivée de client ou changement de paramètre de client est coûteux en ressource de calcul et implique une charge importante de trafic de contrôle pour mettre en œuvre les nouvelles associations calculées.

Une alternative consiste alors à associer seulement les clients qui arrivent au fil de l’eau sans rectifier l’association des clients déjà présents. Cette approche peut néanmoins conduire à une performance sous-optimale. Un compromis doit donc être trouvé entre l’utilisation de ces deux approches (entre qualité de la solution et coût de mise en œuvre).

Pour l'association optimale entre le client et le point d'accès calculée hors ligne (offline), de nombreux travaux formulent l'association en tant que problème d’optimisation tel que celui présenté dans la partie 3.3 dans leur majorité, pour lesquels les travaux dans l’état de l’art proposent des algorithmes heuristiques.

Dans certaines propositions [3], les auteurs supposent que les points d'accès voisins utilisent des canaux orthogonaux qui ne sont donc pas en interférence et peuvent par conséquent communiquer en même temps, et pour d'autres [30], les auteurs supposent des réseaux plus denses dans lesquels les canaux orthogonaux ne sont pas suffisants pour être utilisés entre les points d'accès voisins et les interférences doivent être prises en compte. Ces informations sont présentes au niveau des points d'accès et transmises au contrôleur. Mais dans d'autres situations, le problème est que l'interférence avec un point d'accès adjacent peut ne pas être observée au niveau du point d'accès, alors qu’elle est sensible pour les clients présents dans la zone de chevauchement radio du point d'accès adjacent. Pour cette raison, certains travaux tiennent compte de l'information apportée par les clients, donnant naissance à des travaux basés sur les informations issues des points d'accès et/ou des clients. En outre, dans tous les travaux qui traitent l'association client-AP, la capacité du lien sans fil entre chaque paire client- point d'accès candidat doit être prise en compte. Cette capacité est apprise par l'AP à travers les messages standard échangés [8].

## Les approches distribuées

Dans cette approche, le contrôle peut être effectué par le point d’accès individuellement (qui peut aussi choisir son canal) ou avec une coordination avec les points d’accès voisins, sans vue globale du réseau. Un contrôle distribué peut aussi être fait par les stations clientes qui choisissent de s’associer à un point d’accès, selon un ensemble de critères. La station peut collecter des mesures liées à la performance du réseau avant de sélectionner le point d’accès le plus approprié selon une mesure spécifique [2]. D’autre part, les stations peuvent sélectionner un AP qui maximise leurs métriques d’intérêts potentiels (comme le débit, par exemple). En effet, de nombreuses approches distribuées basées sur les stations ne sont pas conçues pour obtenir un équilibre de charge à l'échelle du système. Cependant, la recherche d'un AP qui fournit la bande passante maximale implique implicitement la sélection du point d’accès le moins surchargé, ce qui est largement utilisé comme heuristique d'équilibrage de charge. Les stations peuvent estimer la surcharge d’un point d’accès de différentes manières. Par exemple, mesurer l'utilisation des canaux par les points d’accès ou le décalage entre le temps estimé d’envoi des *beacons* et celui réellement reçu. De telles approches ne nécessitent aucune assistance du côté réseau [11]. De leur côté, les AP agissent passivement en acceptant les demandes d’association sans restriction particulière tout au long de ce processus de sélection.

# Signalisation lors de l’association des clients aux points d’accès

Comme décrit dans le paragraphe 2, chaque client fait un balayage actif ou passif avant de s’associer à un point d’accès. Une fois cette étape effectuée, la station en question choisit le point d’accès ayant la puissance de signal la plus forte. L’étape qui suit est la demande d’authentification de la station auprès du point d’accès [16,26] à travers le message «Open system authentication request». A la réception du message, le point d’accès répond par le message «Open system authentication response». Lors de la terminaison de l’opération d’authentification, la station envoie le message de demande d’association «association request» auquel le point d’accès répond par le message «association response». La Figure 7 ci-dessous résume les étapes précédentes.

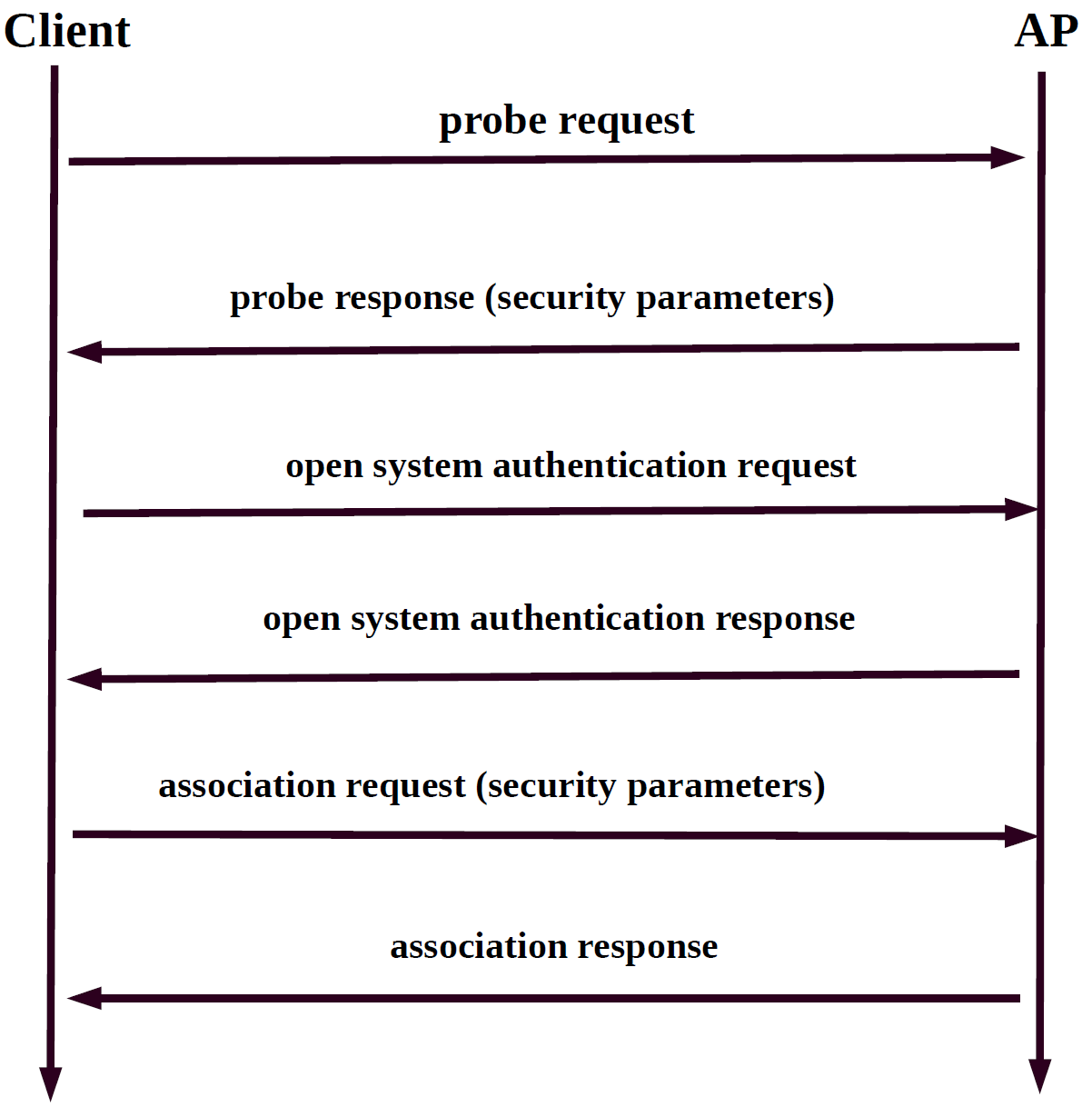
****

Figure 7: L’association entre un Client et un Point d’accès selon la norme 802.11

## Le balayage

Durant le déroulement de cette opération, plusieurs éléments sont utilisés, à savoir:

* le type de balayage, BSSType, qui spécifie si le balayage concerne tous les réseaux ou bien ceux en infrastructure ou ad hoc.
* la station peut balayer tous les points d’accès existants en broadcast, ou bien envoyer le *probe* pour un point d’accès donné en unicast.

D’autres éléments sont aussi présents, tels que le temps d’attente avant le sondage, le délai minimum et maximum avant la fin de la réponse, la liste des canaux à sonder, le nom des SSID à rechercher, le type de balayage actif ou passif.

## Authentification

Si l’authentification RSNA (Robust Security Network Association) est utilisée, l’opération d’authentification peut se dérouler selon trois cas :

* un mot de passe ou un PSK (PreShared Key**)** est utilisé pendant l’opération d’authentification,
* le protocole IEEE 802.1X est utilisé après une authentification à système ouvert (open system authentication)
* ou bien une PSK est utilisée après une authentification à système ouvert.

Dans les trois cas, l’utilisation de RSNA implique que le point d’accès contient un authentificateur et que le client est le demandeur. L’authentification à travers l’adresse MAC du client peut aussi être utilisée après l’utilisation d’un système ouvert.

## Association

Une fois l’opération d’authentification terminée et réussie, l’association permet à la station d’échanger du trafic avec le point d’accès. En effet, une fois l’association acceptée, le point d’accès enregistre la station pour que les trames destinées à cette dernière puissent être acheminées correctement. Le point d’accès répond dans son message «Association response» avec le code 0 en cas de succès et aussi avec le code de l’association (AID: Association ID). Ce code numérique est utilisé pour livrer les trames destinées à la station après leur mise en mémoire au niveau du point d’accès.

# Signalisation Permettant la communication entre les points d’accès et le contrôleur (CAPWAP)

## Objectifs du protocole CAPWAP

On a vu que l’association centralisée reposait sur un contrôleur et un échange de messages de signalisation entre le contrôleur et les AP. Le protocole CAPWAP [17-22] (Control And Provisioning of Wireless Access Points) est une norme standardisée par l'IETF (Internet Engineering Task Force) qui introduit la notion de contrôleur d’AP et permet de les gérer et les configurer. CAPWAP est une évolution du protocole LWAPP (Lightweight wireless Access Point Protocol) [23]. Dans la terminologie CAPWAP, les AP sont appelés WTP (Wireless Termination Point). Les principales fonctionnalités du protocole CAPWAP sont:

* définir les fonctions du contrôleur, en fonction de la répartition des fonctions MAC entre l’AC et les WTP (plus de détail dans le paragraphe suivant),
* configurer les AP du WLAN,
* surveiller le fonctionnement du WLAN,
* contrôler l’accès au réseau et gérer les ressources,
* effectuer les fonctions de sécurité,
* sélectionner les canaux,
* transmettre le trafic des clients vers le contrôleur central AC via le WTP,
* assurer la communication d’informations entre le contrôleur central et les points d'accès, notamment l'état de congestion, les niveaux d'interférences, les taux de perte et les différentes informations sur le délai,
* contrôler les fonctions permettant l'application de la norme 802.11 en pratique (association, roaming, ...), mais en proposant plus de services, tels que la QoS, l’équilibrage de charge, amélioration de sécurité.

De son côté, le contrôleur ou Access Controller (AC) assure les services de gestion suivants :

* le contrôle des listes d'accès (association/ désassociation),
* l'équilibrage de charge (réassociation et distribution),
* la gestion de la QoS,
* la planification,
* la configuration (authentification, dé-authentification),
* la fragmentation/ défragmentation des messages de données et de contrôle.

## Différentes architectures réseaux possibles

Dans la pratique, il existe trois architectures différentes des réseaux802.11 selon le système de distribution utilisé [20]: l'architecture autonome, l'architecture centralisée et l'architecture distribuée. *L'architecture autonome* *WLAN*, où chaque WTP ou AP est configuré individuellement et met en œuvre tous les services 802.11 nécessaires. Dans l'*architecture WLAN distribuée*, pour laquelle les réseaux Mesh sont un bon exemple, les nœuds participants forment un réseau entre eux. Dans l'*architecture WLAN centralisée*, un grand nombre de WTP sont regroupés et gérés par un ou plusieurs contrôleurs, nommés aussi Access Controller (AC).

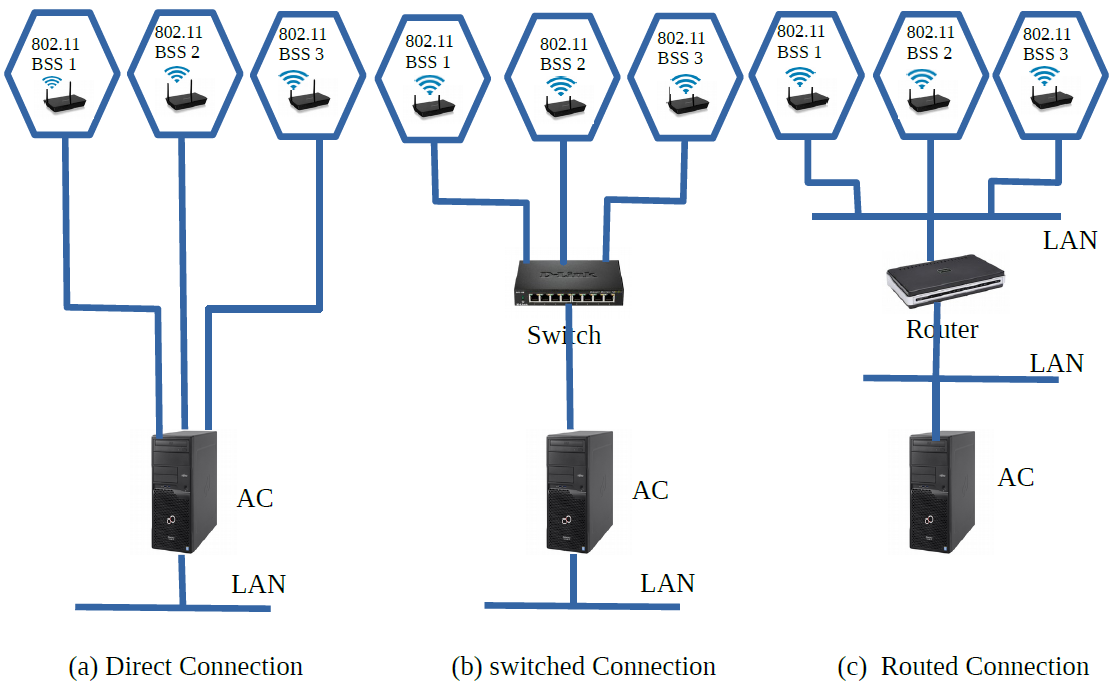


Figure 8: Les différentes connexions entre les WTP et l’AC en architecture centralisée.

En plus de gérer, contrôler et configurer les différents WTP, l'AC peut également effectuer des activités d'agrégation de données. Dans cette architecture centralisée, l'AC peut effectuer une connexion directe avec les WTP, basées sur un commutateur (switch) ou un routeur (router) lors de la connexion des différents WTP, ce qui se traduit par un AC en L2 ou L3 comme illustré dans la Figure 8. Pour assurer l'évolutivité, la redondance et la tâche d'équilibrage de charge, plusieurs AC peuvent être présents ensemble. Dans cette classe de WLAN (centralisée), CAPWAP propose que les fonctions 802.11 puissent être implémentées en partie dans les WTP et/ou l’AC, donnant naissance à des AP légers. Le paragraphe suivant traite de ce point plus en détail.

## Architectures MAC prises en charge par le protocole CAPWAP

Avec CAPWAP, les fonctionnalités MAC 802.11 dans l'architecture centralisée peuvent être réalisées en partie entre le WTP et l'AC. Cette répartition donne naissance à trois classes d'architectures (Figure 9): l'architecture MAC locale (Local MAC), l'architecture MAC fractionnée (Split MAC), et l'architecture MAC distante (Remote MAC). Les trois architectures partagent le fait que la plupart des fonctionnalités CAPWAP sont exécutées par l'AC, tandis que les fonctionnalités de la couche physique 802.11 PHY sont toujours effectuées par le WTP.

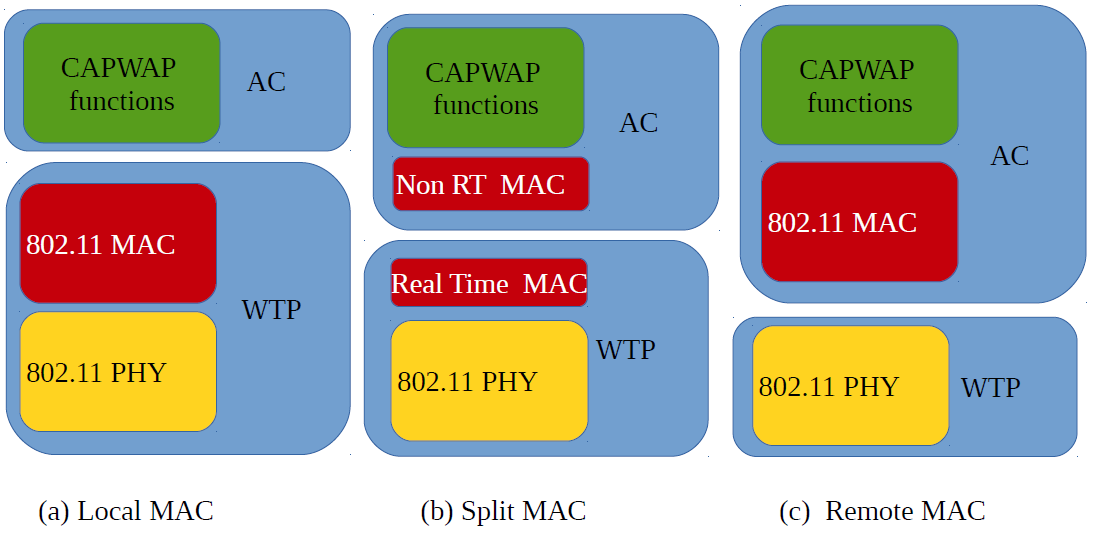


Figure 9: Différentes architectures MAC possibles avec l’architecture réseau centralisée.

### Architecture MAC locale (Local MAC)

Comme dans un AP classique, toutes les fonctionnalités MAC 802.11, notamment celles relatives aux trames des clients, résident dans la WTP, en plus du 802.11 PHY. L'AC gère les WTP en fonction de la politique de gestion réseau.

La configuration du WTP lui-même selon les politiques de gestion réseau est effectuée au niveau de l'AC en communiquant les informations entre le WTP et l'AC. Les fonctionnalités CAPWAP sont impliquées dans leur majorité au niveau AC, à part celles liées à l'état des canaux que le WTP retransmet en plus des statistiques reliées aux clients.

### Architecture MAC fractionnée (Split MAC)

Comme son nom l'indique, dans cette classe, les fonctionnalités MAC sont divisées entre le WTP et l’AC. En fait, l'entité WTP implémente les services MAC 802.11 temps-réel et la gestion de la radio, tandis que les services non temps-réel, la gestion des autres contrôles (authentification, QoS,...) ainsi que les trames de données sont effectuées par l'AC de manière centralisée, en plus de la gestion des WTP eux-mêmes (exemple: reconfiguration si nécessaire).

Le contrôle de la radio reste au niveau du WTP lui-même afin de décharger l'AC et lui permettre de gérer un grand nombre de WTP. Pour des raisons d’efficacité, le WTP est chargé de la gestion temps réel comme la génération de *beacons*, la transmission des *probe response*, les retransmissions de trames de données, l'adaptation des débits, la synchronisation et le traitement des trames de contrôle (RTS, CTS, ACK ...). La réassociation est également considérée comme un service temps-réel pour certaines applications, et peut donc être implémentée sur le WTP. L'exécution des autres tâches par l'AC permet de réduire la complexité et donc le coût des WTP.

En outre, le fait d'effectuer les tâches de chiffrement/ déchiffrement au niveau de l’AC diminue la possibilité de failles de sécurité sur le WTP car il ne gère pas les clés de chiffrement des utilisateurs. De plus, l'amélioration ou mise à jour des algorithmes de chiffrement aura un coût limité car le WTP n'est pas concerné et la modification est effectuée uniquement au niveau AC. Les fonctions AC peuvent être effectuées par des machines AC différentes si elles sont utilisées ensemble, par exemple une machine AC sera responsable de la tâche plan de contrôle, et une autre pourra être dédiée au plan de données.

### Architecture MAC distante (Remote MAC)

Dans cette classe d'architectures MAC, toutes les fonctions MAC 802.11 résident dans l'AC et le WTP joue le rôle d'un relais entre les clients et l'AC et n’assure que la couche physique. Toute la complexité est située dans l’AC puisque tant les fonctions CAPWAP que les fonctions à caractère temps-réel résident dans l'AC. Comme les tâches temps-réel sont contenues dans l'AC, des dispositions spéciales devraient être effectuées pour diminuer le délai entre le WTP et l'AC tels que le câblage qui doit avoir un débit élevé (utiliser la fibre optique par exemple).

## Interface de communication entre WTP et AC

Lors de l’initialisation, le WTP doit découvrir l'AC dont il va ensuite dépendre. Cette opération peut être effectuée de manière statique ou dynamique. Après cette étape de découverte, une authentification est effectuée entre le WTP et l'AC, de sorte que le WTP s'authentifie auprès de l'AC et par mesure de sécurité, elle peut être réciproque. Une fois l’authentification réussie, le WTP s'associe à l'AC, télécharge le firmware à utiliser puis établit un canal de contrôle pour communiquer les trames decontrôle et de gestion. Après cet établissement de canal, l'AC envoie les paramètres de configuration au WTP. La Figure 9 ci-après résume les étapes principales de l’association et de fonctionnement du protocole CAPWAP entre le WTP et l’AC.

Un canal de contrôle CAPWAP est un canal bidirectionnel permettant aux paquets de contrôle CAPWAP d’être transmis et reçu. Il est défini par les adresses IP de l’AC et du WTP, les ports de contrôle utilisés au niveau de l’AC et de WTP et aussi du protocole de transport utilisé. De plus, un canal de données CAPWAP pour envoyer et recevoir les données est défini sur un port différent du canal de contrôle. Les paquets de contrôle CAPWAP, et optionnellement ceux de données sont sécurisés en utilisant le protocole de transport DTLS (Data Transport Layer Security) [24]. Les messages de données CAPWAP encapsulent les trames renvoyées par le WTP à l’AC, tandis que les messages de contrôle sont ceux de gestion échangés entre l’AC et le WTP.

Le protocole CAPWAP comporte 4 phases (Figure 9) : découverte (optionnelle), connexion sécurisée, configuration et communication.

Au début du protocole CAPWAP, le WTP découvre les AC disponibles en envoyant un message de demande de découverte «Discovery request», pour lequel les AC répondent avec un message «Discovery response». Le WTP peut se passer de la phase de découverte des AC s’il a un AC déjà enregistré a son niveau et il veut l’utiliser, on parle alors d’une configuration statique de l’AC au niveau du WTP.

Le WTP choisit un AC avec lequel une connexion DTLS sera établie. Les certificats DTLS doivent être disponibles pour permettre l’authentification. Après l’établissement de cette connexion, on fait un échange de messages pour la configuration et l’accord sur la version à utiliser.

Une fois que le WTP a fourni sa configuration à l’AC à travers le message «Configuration Status Request», l’AC de son côté doit envoyer sa configuration au WTP par le message «Configuration Status Response». Cela permet au WTP de recevoir les politiques de l'AC. Dans la Figure 9, l’image de la firmware est supposée disponible au niveau du WTP, par contre si ce n’est pas le cas, le WTP demande à l’AC de lui envoyer l’image de la version utilisée.

Les messages de contrôle CAPWAP, tels que le message «WTP Event Request» envoyé par le WTP, indiquent à l’AC que le WTP est opérationnel. Lorsque de tels messages de contrôle ne sont pas envoyés, les messages «Echo Request» (envoyé par le WTP) et «Echo Response» (envoyé par l’AC) sont utilisés pour maintenir la communication du canal de contrôle. A défaut de réception d’un de ces messages, l’AC considère le WTP comme non opérationnel. De son côté, le WTP s’il ne reçoit pas de message ou de réponse de la part de l’AC, il le suppose défaillant et tente de découvrir un nouvel AC.

Le protocole CAPWAP transmet les commandes de l'AC au WTP afin de gérer les stations qui communiquent avec le WTP. Cela inclut la création de structures de données locales dans le WTP pour les stations et la collecte d'informations statistiques sur la communication entre le WTP et les stations. CAPWAP fournit un mécanisme à l'AC pour obtenir les informations statistiques collectées par le WTP. Dans le tableau 2 qui est dans l’annexe, on présente quelques messages échangés entre le WTP et l’AC.

Le protocole CAPWAP effectue un modèle standard de liaison entre le WTP et l’AC indépendant de la technologie de communication utilisée entre le WTP et les stations, et mise en place dans les deux composants. Cette liaison standard s’adapte pleinement à la technologie 802.11 comme à d’autres (WIMAX par exemple) en appliquant des changements appropriés à la technologie (paragraphe 5.5). Les messages utilisés spécifiquement pour une technologie donnée commencent par son nom, comme par exemple dans le paragraphe qui suit, les messages commencent par 802.11, puisque c’est la technologie qu’on utilise dans notre projet «smart AP» entre le WTP et les stations. La Figure 10 ci-dessous montre l’échange de messages entre le WTP et l’AC pour l’établissement de la connexion. A la fin de l’échange de messages, et si aucune erreur ne s’est produite, le WTP et l’AC sont bien authentifiés et peuvent échanger les messages de contrôle CAPWAP.

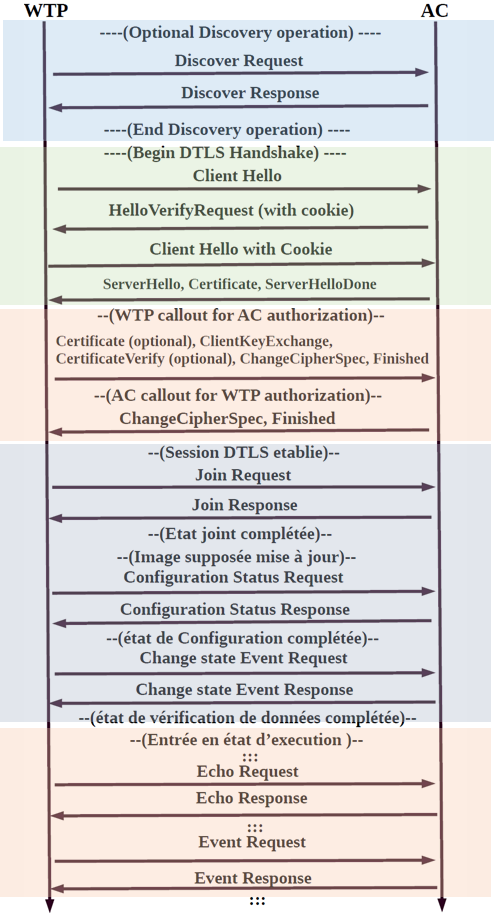


Figure 10: Échange de messages de protocole CAPWAP

## Les liaisons avec 802.11

Le protocole CAPWAP assure la liaison entre le WTP et l’AC indépendamment de la technologie radio utilisée entre le WTP et le client, a savoir WIMAX, WIFI.... Pour l’utilisation avec la norme IEEE 802.11, CAPWAP configure spécifiquement la norme 802.11 en plus de la partie commune pour toutes les technologies, pour prendre en charge les fonctions requises du protocole IEEE 802.11.

Afin de permettre la prise en charge de la norme 802.11 (la liaison), deux messages seront échangés entre le WTP et l’AC, à savoir, le message de demande de configuration (802.11 WLAN configuration request) et la réponse à ce message (802.11 WLAN configuration response).

La demande de configuration WLAN IEEE 802.11 est envoyée par l'AC au WTP pour modifier les services déjà fournis par le WTP, ou pour en créer un nouveau réseau WLAN. La modification de service peut se faire manuellement, par l’administrateur, et peut consister par exemple aussi à supprimer un WLAN déjà existant. La création d’un WLAN se fait suite à l’envoi d’une demande de configuration par le WTP à l’AC à travers le message «Configuration Update Response». De son côté, le WTP après le changement des services comme demandé par l’AC, renvoie une réponse à ce message qui est «IEEE 802.11 WLAN Configuration Response» ou même pour mentionner une erreur lors de l’application des changements requis dans la demande de l’AC.

Le tableau 3 en annexe résume différents éléments utilisés dans les messages de contrôle et qui sont destinés pour la prise en charge de la norme 802.11.

### LOCAL MAC

Comme indiqué dans le paragraphe sur les architectures MAC CAPWAP avec Local MAC, les trames de données sont directement ponctuées et formatées sous forme de trames 802.3 par le WTP. Les trames de contrôle sont traitées localement par le WTP avant d’être transmises à l’AC.

En mode MAC local, le service d'intégration est activé au niveau du WTP, alors que le service de distribution peut l’être au niveau du WTP ou de l’AC. Lorsqu'il est effectué au niveau de l’AC, le WTP doit formater les trames générées par la station sous forme de trames 802.3 avant de les fournir à l’AC. Malgré l’activité MAC de l’association est terminée au niveau du WTP, mais l’AC doit être informé des événements de mobilité, envoyés à travers les demandes d’associations (trames 802.11 association request) et peut aussi interdire la nouvelle association envoyée par le WTP, en répondant par une trame 802.11 «association failure response», et le WTP envoie de son coté à la station une demande de dé-association (à travers la trame de dé-association). Aussi, le WTP doit renvoyer toutes les trames de gestion des clés IEEE 802.1X, EAP et RSNA à l’AC (depuis la station), et renvoyer à la station les réponses correspondantes de l’AC. Cela implique que le client AAA est implanté au niveau de l’AC.

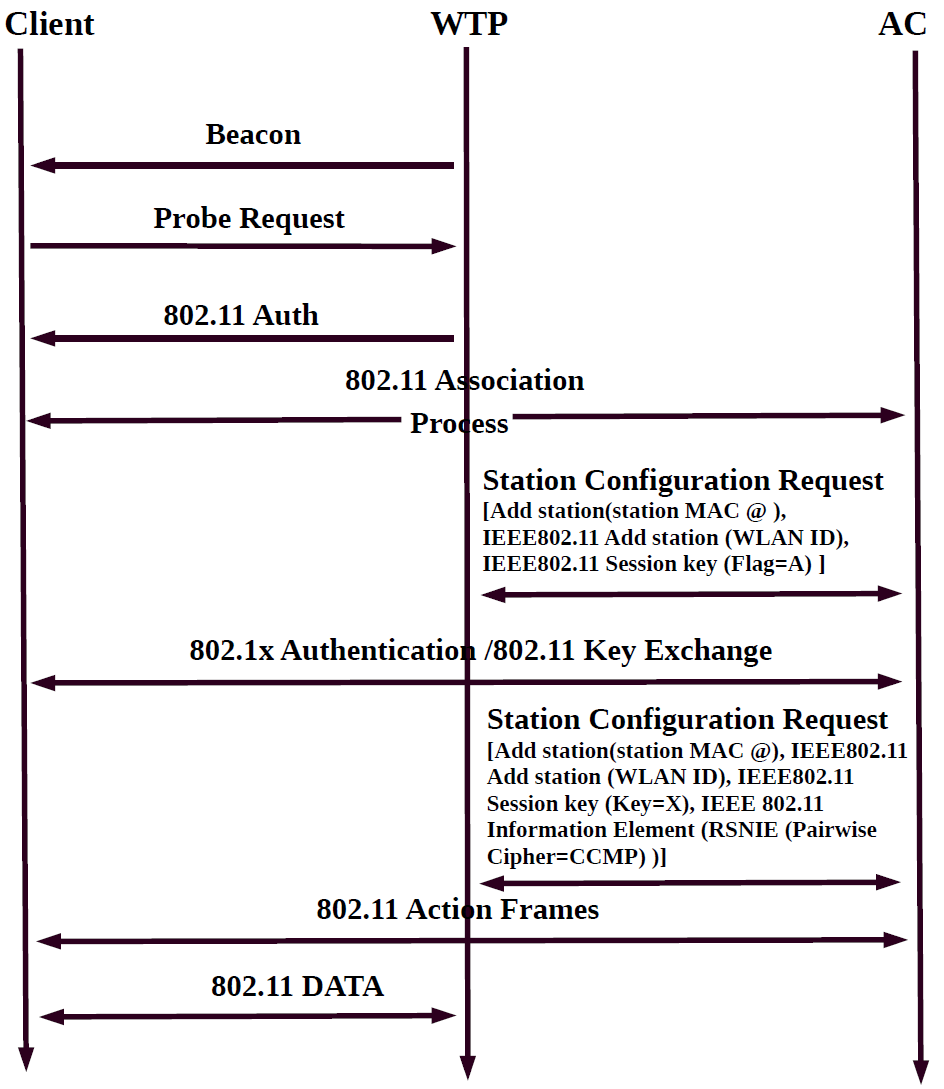


Figure 11: Les flux de messages avec Local MAC

Le WTP génère les trames beacons IEEE 802.11, traite les trames de demande de sondage (Probe request) envoyées par les stations et répond avec une trame de réponse de sonde correspondante (probe response). Le WTP renvoie les trames 802.11 d’authentification et d’association à l’AC pour décider de l’acceptation ou pas de cette association. Si l’association est acceptée, l’AC envoie une demande de configuration de la station (station configuration request) avec l’élément de demande de l’ajout de la station au WTP. Le WTP renvoie toutes trame de gestion d’action, reçue depuis la station, à l’AC, alors qu’il peut jouer le rôle de passerelle pour les messages de données envoyés par le client, en effectuant le chiffrement/ déchiffrement nécessaires ou bien aussi le rôle de tunnel en utilisant le mode 802.3 ou 802.11. La Figure 11 montre le déroulement de l’association en architecture local MAC.

### SPLIT MAC

Dans une architecture MAC fractionnée, les services de distribution et d'intégration sont assurés par l’AC et toutes les données des utilisateurs sont transmises en tunnel entre le client et l’AC à travers le WTP. Comme indiqué dans le paragraphe de l’architecture Split MAC, les fonctionnalités MAC en temps réel, tels que la génération de beacons et les réponses aux trames de découvertes (probe response) sont effectuées par le WTP. Tandis que les autres fonctionnalités sont assurées au niveau de l’AC, tel que la trame de demande d’association (association request). En effet, lorsque le WTP répond à la station par la trame de réponse, il renvoie aussi la demande (probe request) à l’AC pour qu’il décide de l’association. Aussi, le WTP renvoie la trame 802.11 d’authentification et d’association à l’AC. L’AC de son coté, envoie au WTP une demande de configuration de la station (configuration request message) après que l’association avec la station est complétée, afin que le WTP rajoute la station. Si le WTP assure les fonctionnalités de chiffrement/ déchiffrement, une autre demande est envoyée par l’AC qui contient les informations de clé de chiffrement, tandis qu’un message indiquant que c’est lui qui va faire l’opération de chiffrement/ déchiffrement (le flag ‘c’ activé). Aussi, le WTP renvoie toute trame de gestion d’action à l’AC et assure le tunnel pour les messages de données entre l’AC et la station. La Figure 12 ci-dessous montre le déroulement de l’opération d’association d’un client en architecture MAC Split.

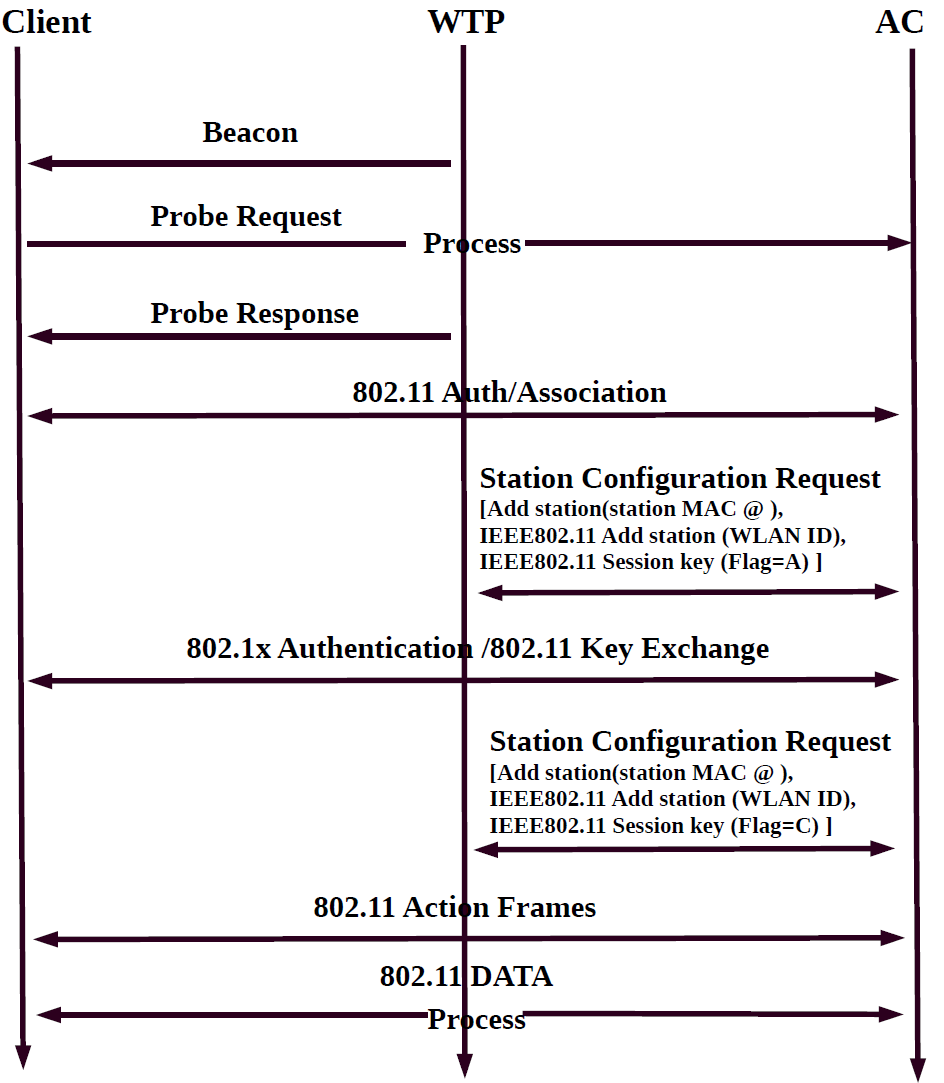


Figure 12: Les flux de messages avec Split MAC

### La procédure de changement de WTP (Roaming)

Un client qui est associé d’une manière sécurisée avec un WTP, peut effectuer une opération de changement de WTP suite à une mobilité (roaming). La Figure 13 montre le déroulement de cette opération en utilisant le protocole de contrôle CAPWAP d’une manière sécurisée. Dans l’exemple de la figure, les services cryptographiques sont fournis par le WTP. Si c’est l’AC qui doit assurer ce service, la dernière étape de demande de configuration de station serait différente.

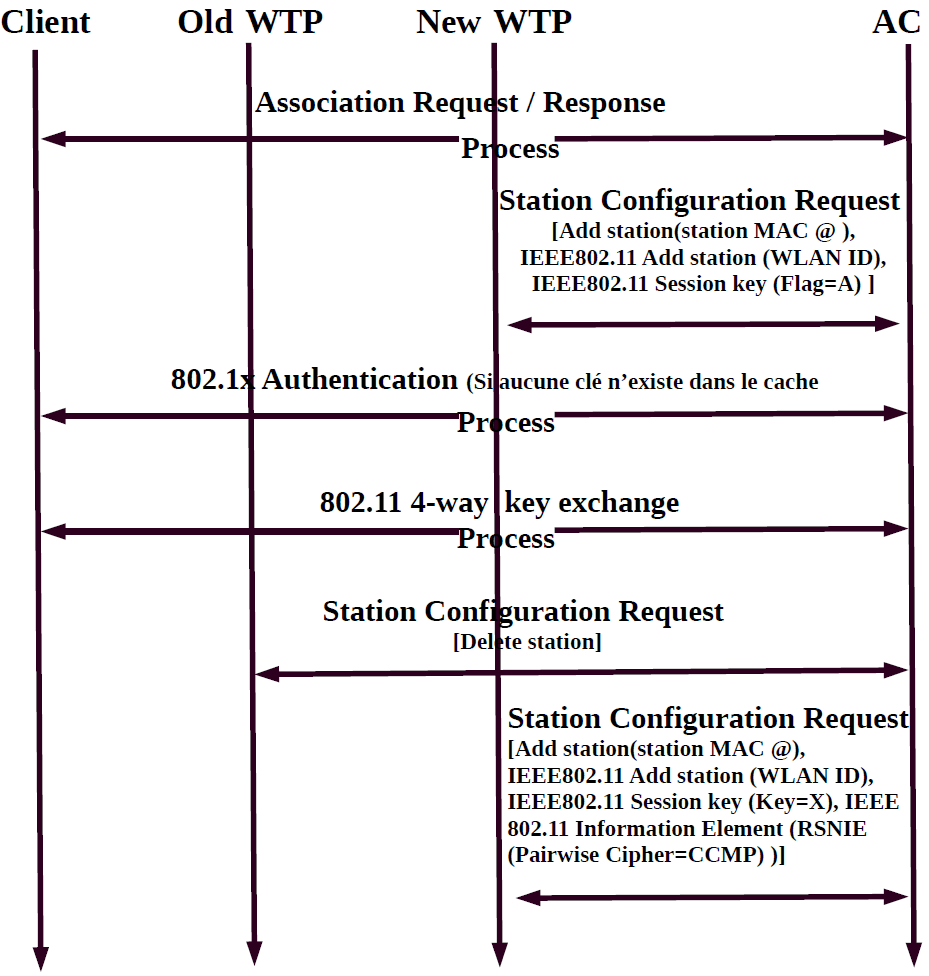


Figure 13: Déroulement d’une opération de Roaming

# Changement de point d’accès transparent aux clients (Roaming déclenché par l’AP)

Dans les parties 2 et 3 nous nous sommes intéressés à des techniques de l’état de l’art permettant de donner des critères pour une association optimisée des clients au AP, mais sans détailler la mise en œuvre de telles associations. ODIN [25] est une architecture qui permet cette mise en œuvre. Il permet de changer l’association d'un client à un point d'accès donné d'une manière transparente pour le client. C’est-à-dire sans se soucier de la cause de ce changement d’association côté client, qui pourrait être due à la force du signal, ou encore à des raisons de qualité de service.

ODIN propose une plateforme de contrôle centralisée qui gère l'ensemble des points d’accès. Chaque client est associé à un point d'accès virtuel unique (LVAP: Lightweight Virtual Access Point) dédié au client (BSSID unique). Ce point d’accès virtuel est le seul visible par le client. Il s’instancie dans divers AP physiques en fonction de l’association souhaitée.

En effet, chaque AP physique gère un ensemble de LVAP correspondants aux clients connectés, cela se fait de manière similaire à un ensemble de clients logiquement isolés connectés à différents ports d'un même commutateur. En pratique, à chaque fois qu'un nouveau client arrive sur le réseau, il analyse les points d’accès disponibles de proximité en générant un message de requête de sondage (probe request) pour lequel les AP répondent et deviennent des candidats-associés. Le client choisit un AP de la manière standard et commence la procédure de prise de contact qui se transforme avec ODIN en une abstraction LVAP comme décrit précédemment. Les messages de contrôle entre le client et le LVAP sont échangés en unicast afin d'isoler chaque client des autres. ODIN permet de réaliser différents types de services tels que l'équilibrage de charge, la gestion de la mobilité, la détection de brouillage (jamming detection), la sélection automatique des canaux et la gestion de l'énergie. La Figure 14 montre une architecture possible et un exemple de fonctionnement d’ODIN.

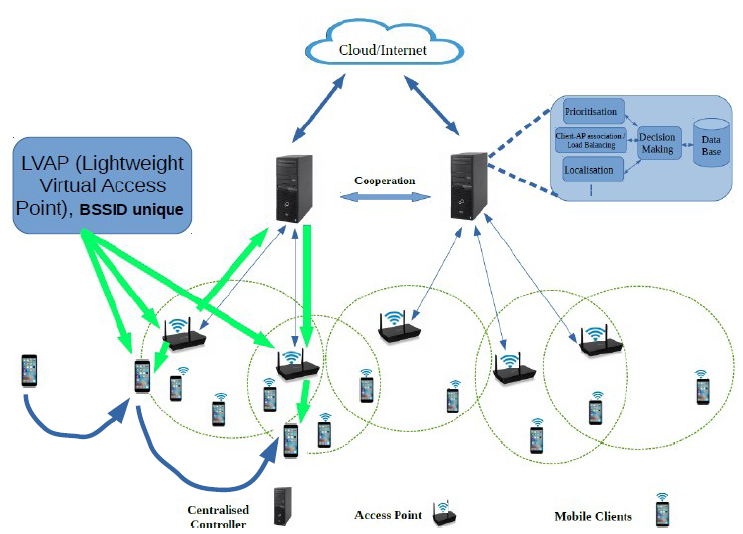
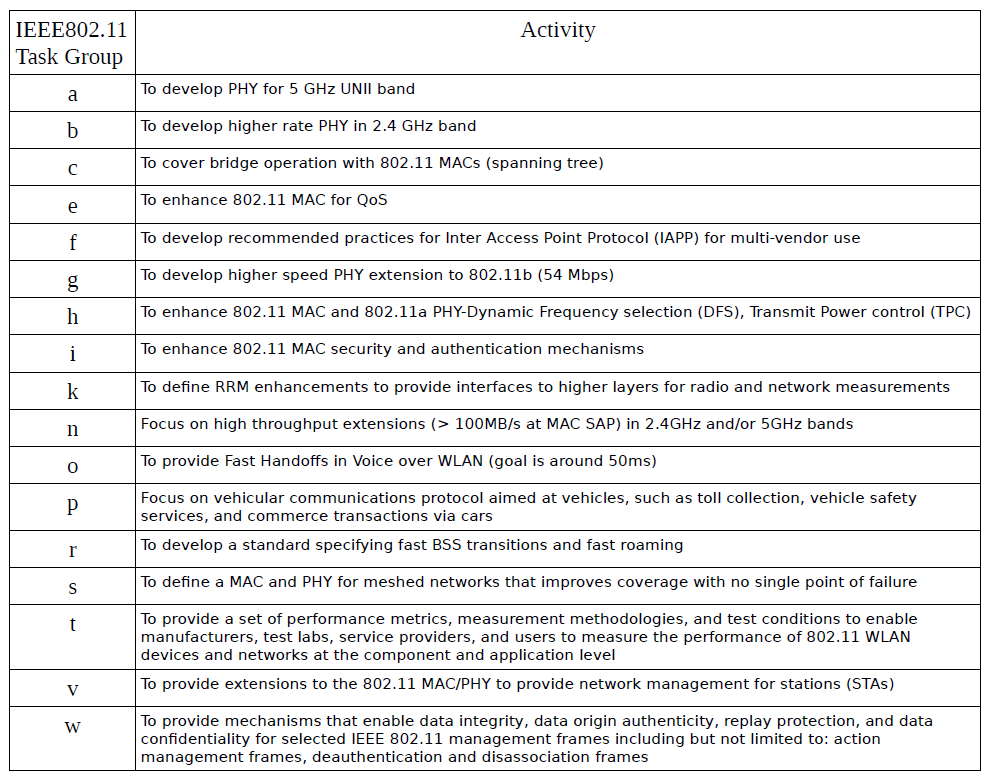


Figure 14: Architecture décrivant le fonctionnement de ODIN

# Quelques travaux des groupes IEEE 802.11 et leurs améliorations

Depuis sa première adoption en 1997, la norme 802.11 ne cesse d’évoluer proposant ainsi l’utilisation des bandes de fréquences de 5 GHz (norme a et n) ou de 2.4GHz (norme b, g, n), ou intégrant de nouveaux aspects, tels que la Qualité de service (802.11e), la sécurité (802.11i), les communications véhiculaires (802.11p)… Dans ce paragraphe, quelques amendements sont présentés, qui ont une relation avec le projet de notre étude et le tableau 1 ci-dessus résume le travail de quelques groupes IEEE 802.11 [12].



**Tableau 1: Quelques amendements de la norme 802.11**

## 802.11e,MAC amélioration concernant la qualité de service (QoS)

L’amendement 802.11e [13, 14] est une amélioration du MAC 802.11b pour offrir une qualité de service différenciée. Dans cet amendement, le standard définit une fonction de coordination hybride (HCF), qui permet à la fois d’avoir un accès au canal en mode de contention et un accès sans contention. Pour permettre l’accès en mode sans contention, une amélioration de la fonction DCF (Distributed Contention Function), appelée EDCA (Enhanced Distributed Channel Access), propose de différencier le service à travers un accès priorisé au canal définissant ainsi des catégories d’accès (CA). En effet, chaque station possède quatre catégories, pouvant chacune avoir plusieurs valeurs de priorités. On peut considérer chaque catégorie comme étant une station virtuelle à l’intérieur de la station elle-même, possédant aussi sa propre file d’attente avec les paramètres de priorités et effectuant les opérations de contention et de backoff indépendamment des autres catégories CA au sein de la même station. Dans la Figure 15 suivante, le schéma montre la gestion possible des différentes files.

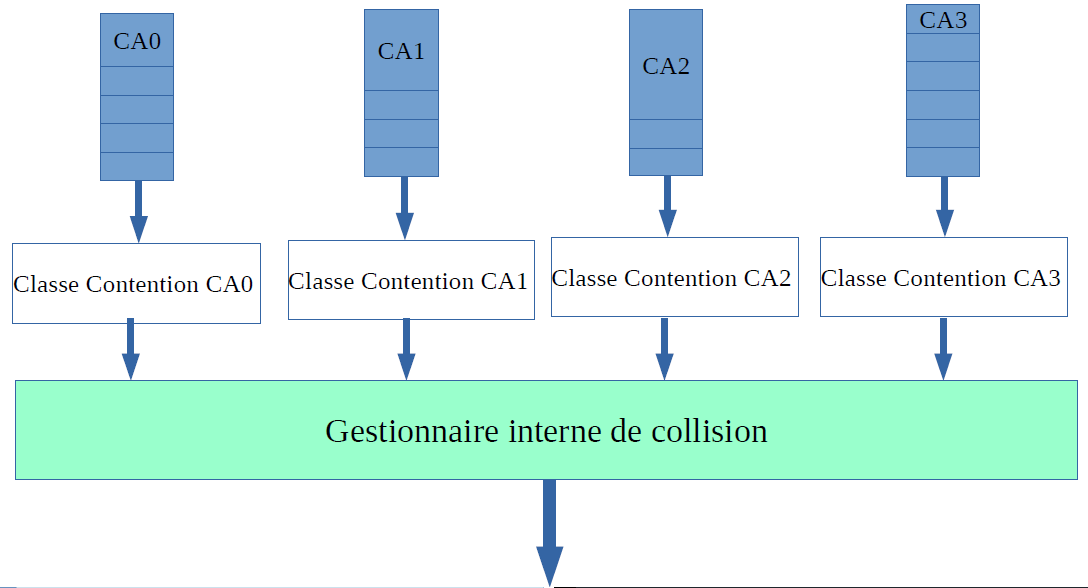


Figure 15: Gestion files d’attentes des différents AC dans 802.11e

Avec EDCA, l'accès différencié au canal est réalisé par la variation de la taille de la fenêtre de contention ainsi qu’au temps passé en détection de canal occupé, en définissant 8 priorités d’utilisateurs différentes, englobés par les 4 catégories d’accès. Dans DCF du 802.11b, les nœuds doivent détecter que le canal est inactif pour une période DIFS (Distributed Inter Frame Space) avant de tenter de transmettre. En 802.11e, le DIFS est remplacé par le temps arbitraire entre trames AIFS (Arbitrary Inter-Frame Space). La classe CA ayant la plus haute priorité possède le plus petit AIFS et celle ayant la priorité la plus basse possède le plus grand AIFS. Cela a pour but de donner plus de chance à la classe plus prioritaire d’accéder rapidement au canal. De plus, la taille de la fenêtre de contention, qui détermine le temps d’attente (backoff) avant d’essayer d’accéder au canal, varie pour chaque AC. La valeur de cette fenêtre commence par une valeur minimale (CWmin) et double à chaque échec (retransmission) jusqu’à atteindre sa valeur maximale (CWmax). En pratique, les classes CA ayant une priorité plus élevée ont des valeurs CWmin et Cwmax plus petites pour permettre un accès au canal plus rapidement.

## 802.11k, radio resource measurement

Le but de cet amendement est d’offrir des informations concernant l’état des ressources radio afin d’être utilisée pour augmenter les performances des stations et donc de tout le réseau. En effet, les applications comme la voie et la vidéo sur IP, la localisation nécessitent des informations exactes sur les mesures radio afin de fonctionner correctement. Cet amendement permet d’avoir ces informations sous formes de demandes nécessitant des réponses, aussi sous formes de rapport (sans être demandé) ou bien même sous forme de demandes sans nécessité de réponses [12,15,16]. Chaque information sera disponible avec l’identifiant de l’objet (OID: Object IDentifier) dans la MIB (management information base) pour permettre l’interfaçage avec les couches supérieures.

Les stations peuvent faire les mesures radio localement, demander aussi ces mesures à d’autres stations dotées de l’amendement ou bien aussi être demandés par d’autres stations pour effectuer les mesures radio et rendre le résultat. Ces informations peuvent par exemple être utiles en cas d’opérations de changement de points d’accès lors de la mobilité, tels que la charge des canaux et l’état des points d’accès voisins. La délivrance de telles informations peut réduire sensiblement le temps de handover entre les cellules et permettant aux stations concernées de choisir d’une manière intelligente la façon d’optimiser les ressources tel que l’énergie et le débit. Les différentes informations couvertes par cet amendement sont présentées dans l’annexe.

## 802.11r, fast basic service set transition

Le but de cet amendement est de permettre des transitions rapides entre deux cellules BSS (Basic Service Set) appartenant au même ensemble ESS (Extended Service Set) pour minimiser la période de déconnexion [15].

En pratique, la migration d’une station du point d’accès actuel auquel elle est associée, au nouveau point d’accès nécessite plusieurs étapes. La première étape consiste à découvrir les points d’accès du voisinage, la deuxième permet d’effectuer la phase d’authentification avec le point d’accès choisi, mais elle consomme beaucoup de temps. De ce fait, le but de l’amendement 802.11r est de minimiser ce temps d’authentification tout en gardant le même niveau de sécurité que celui offert par la norme 802.11i et aussi les mêmes options concernant la QoS que celles offertes par 802.11e. En effet, la négociation des paramètres est faite avant la réassociation, ce qui permet d’accélérer la nouvelle association. Cela est appelé la transition rapide FT (Fast Transition) et concerne le cas des points d’accès appartenant au même ESS, aussi appelé le domaine de mobilité.

En outre, l’amendement 802.11r permet à la station de faire un handshake FT à 4 étapes dès la première association, permettant aussi d’établir un mécanisme de gestion de clés pour l’ensemble du domaine de mobilité ce qui anticipera l’opération d’authentification au cas de migration du point d’accès actuel vers le nouveau point d’accès. Lors de la prochaine transition, la station négocie l’authentification et la QoS avec le nouveau point d’accès selon deux protocoles FT qui sont FT et FT avec demande de ressource (Resource request), selon que la station nécessite une réservation de ressources pour QoS ou pas, conformément à l’amendement 802.11e. En d’autres termes, lors d’un roaming d’un AP à un autre, on doit s’assurer que le nouvel AP assure aussi les fonctions 802.11e et faire les réservations de ressources en conséquence.

## 802.11v, Wireless network management:

Cet amendement permet aux stations d’échanger des informations permettant l’amélioration de l’utilisation des ressources de réseau [15,16]. Les stations sont par conséquent au courant des ressources et de la topologie du réseau. Elles ont également connaissance des interférences du voisinage, et par la suite elles vont gérer les paramètres des ressources radio selon les conditions réelles du réseau. Cet amendement permet aussi aux stations d’échanger des informations sur leur localisation. Pour mieux gérer la consommation d’énergie, l’amendement 802.11v permet aux stations d’être en mode sleep, et ne pas recevoir les trames de l’AP. Cet amendement peut être vu comme suite ou complément de l’amendement 802.11k, qui lui aussi fournit des mesures sur l’état des ressources réseaux, mais la norme 802.11v offre plus de services et d’informations. Dans l’annexe, un résumé sur les différents services et mécanismes qu’offre l’amendement est décrit.

# Bilan

Avec l’utilisation importante des réseaux WLAN et leurs densifications, une gestion globale des différents points d’accès devient indispensable afin d’optimiser le débit et la qualité de service du réseau.

Dans ce livrable, nous avons présenté le mécanisme standard d’association des clients aux points d’accès. Nous avons ensuite présenté quelques classes de travaux qui ont comme but l’optimisation de l’association, à travers quelques paramètres importants tels que l’équilibrage de charge et l’augmentation de débit global. Aussi, nous avons présenté la signalisation standard 802.11 utilisée pour une association simple (client-point d’accès), ainsi qu’un protocole standardisé, appelé CAPWAP, qui vise à gérer différents points d’accès par un même contrôleur. Nous avons également présenté ODIN qui permet de changer les associations des clients aux points d’accès d’une manière transparente pour les clients, évitant ainsi toute modification logicielle de ces derniers.

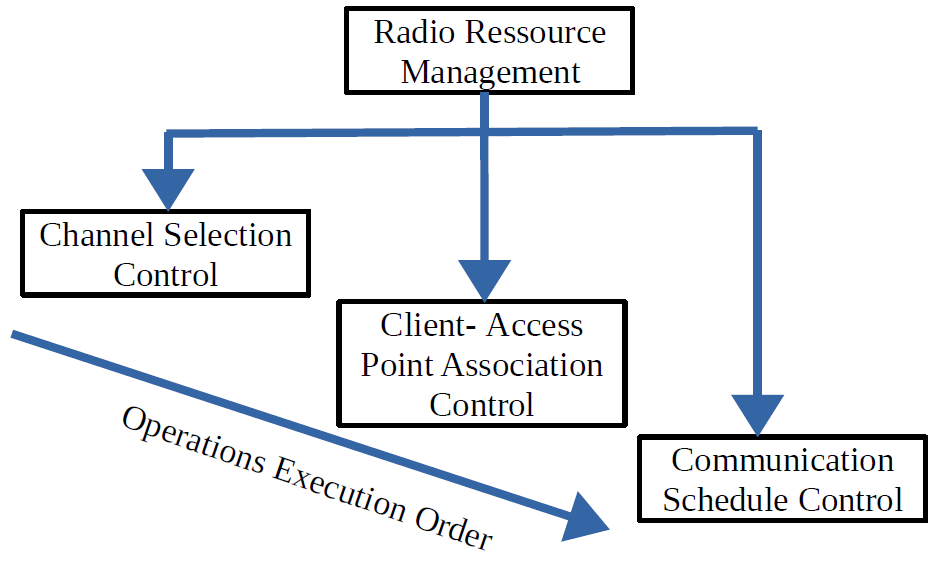


Figure 16: Les axes essentiels pour optimiser les ressources radio

Afin d’améliorer le débit global du réseau WLAN ainsi que celui des clients d’une manière individuelle, trois axes principaux pour la gestion des ressources radio dans les WLAN peuvent être optimisés. À savoir, comment sélectionner les canaux de communication sans fils des différents points d’accès, puisque le déploiement dense des points d'accès donne naissance à un réseau multicellulaire pour lequel les canaux interférents doivent être contrôlés afin de permettre une meilleure réutilisation spatiale. Le deuxième axe est l’association des clients aux points d'accès afin d'optimiser l'utilisation de la capacité physique de chaque point d’accès et chaque client. Le troisième domaine est la planification des communications afin d'éviter toute interférence entre les cellules et à l’intérieur de chaque cellule. Un quatrième axe qui pourrait être utilisé conjointement avec les trois domaines précités est le contrôle de puissance des communications qui aide à mettre en pratique les autres aspects de la gestion des ressources radio. En résumant, avant l'utilisation d'un WLAN multicellulaire, les différents points d'accès devraient sélectionner leurs canaux à utiliser. Les clients après cela s'associent aux points d'accès en fonction d'un paramètre à optimiser. En se basant sur ces associations, les communications sont programmées d'une manière coordonnée ou aléatoire. Une optimisation conjointe des étapes précédentes pourra également être envisagée. La Figure 16, ci-dessus, résume ces axes de recherche.

Annexes

# A1 Interface de communication entre WTP et AC selon le protocole CAPWAP

Dans le tableau 2 qui suit, quelques messages échangés entre le WTP et l’AC pour la mise en place du protocole CAPWAP sont présentés:

|  |  |  |  |
| --- | --- | --- | --- |
| Message requête | Message réponse | Echange | Objectif |
| Discovery request | Discovery response | WTP → AC | découvre les ACs disponibles |
| Configuration Status Request | Configuration Status Response | WTP → AC | fournir la configuration dans le request, et recevoir celle de l’AC dans le response |
| Configuration Update Request | Configuration Update Response | AC → WTP | demander de changer sa configuration. La réponse contient le code de mise à jour |
| WTP Event Request | WTP Event response | WTP → AC | envoyer périodiquement, ou suite à un événement asynchrone. Il indique que le WTP est opérationnel, et aussi pour transmettre les statistiques récoltées. |
| Change State Event Request | Change State Event Response | WTP → AC | indiquer à l’AC la prise en compte de la mise à jour radio si après réception de «Configuration Status Response». Il indique une modification inattendue de l'état opérationnel de la radio si envoyé pendant l’exécution. L’AC modifie les structures de données du WTP comme nécessaire. |
| Echo Request | Echo Response | WTP → AC | maintenir la communication du canal de contrôle, sinon le canal est considéré non opérationnel |
| Clear Configuration Request | clear Configuration Response | AC → WTP | réinitialiser la configuration radio du WTP à celle de fabrication par défaut |
| Image Data Request | Image Data response | AC←→  WTP | s’assurer de la bonne version et au cas contraire mettre à jour la firmware sur le WTP. Le processus continue sous forme de requête et réponse contenant les paquets de firmware jusqu’à la réception de la fin de fichier |
| Reset Request | Reset Response | AC → WTP | demander le redémarrage du WTP. |
| Data Transfer Request | Data Transfer Response | AC←→  WTP | envoyer les données réelles ou de débogage. l’envoie du fichier est sous forme requête -réponse, jusqu’à la fin du fichier. Il peut se faire à l’initiative du WTP ou de l’AC. |
| Station Configuration Request | Station Configuration Response | AC → WTP | Sert à créer, modifier ou supprimer une session d’une station sur un WTP. Des éléments peuvent être contenus dans le message et concernent «add station», ou «delete station» |

Tableau 2: Quelques messages de communication entre AC et WTP

# A2 Les liaisons du protocole CAPWAP avec 802.11

Le tableau 3 ci-dessous présente un résumé sur différents éléments utilisés dans les messages de contrôle CAPWAP et qui servent à la prise en charge de la norme 802.11.

|  |  |  |
| --- | --- | --- |
| Élément | Sens | Objectif |
| IEEE 802.11 Add | AC → WTP | Définit un WLAN sur le WTP |
| IEEE 802.11 delete | AC → WTP | informe le WTP de la suppression du WLAN |
| IEEE 802.11 antenna | WTP → AC | fournit des informations sur les antennes disponibles |
| IEEE 802.11 assigned BSSID | WTP → AC | réponse à la demande de création de WLAN par l’AC. La valeur de BSSID est choisie par le WTP. |
| IEEE 802.11 Direct Sequence  Control | AC ←→ WTP | Si envoyé par l’AC, le WTP doit respecter les directives incluses. Si envoyé par le WTP, il contient l’état actuel (802.11b) |
| IEEE 802.11 MAC Operation | AC → WTP | définit les paramètres MAC sur le WTP |
| IEEE 802.11 MIC Countermeasures | WTP → AC | Indique une défaillance MIC |
| EEE 802.11 Multi-Domain Capability | AC → WTP | Informe le WTP des limites réglementaires en transmettant un message par bande de fréquences pour indiquer les contraintes. |
| IEEE 802.11 OFDM Control | AC ←→ WTP | Concerne seulement la norme 802.11a. Si utilisé par l’AC, le WTP doit respecter les valeurs envoyées. Si envoyé par le WTP il inclut l’état actuel. |
| rate set | AC → WTP | mentionne les débits opérationnels pris en charge |
| IEEE 802.11 Supported Rates | WTP → AC | Indique les débits qu'il peut accepter |
| IEEE 802.11 RSN Error Report | WTP → AC | Mentionne les erreurs de la station, envoie en cas d’erreurs |
| IEEE 802.11 Station | AC → WTP | Accompagne l'élément «add station» et réalise la politique IEEE 802.11 de la station. |
| IEEE 802.11 Station Session Key | AC → WTP | Fournit des clés de chiffrement ou pour configurer une politique d'accès sur le WTP. |
| IEEE 802.11 Statistics | WTP → AC | Transmet les statistiques à l’AC |
| IEEE 802.11 Tx Power | AC ←→ WTP | Si envoyé par l’AC, indique la puissance d’émission que le WTP doit utiliser. Si envoyé par le WTP, contient le niveau de puissance actuel de la radio du WTP. |
| IEEE 802.11 Tx Power level | WTP → AC | communique les niveaux de puissance qui prend en charge |
| IEEE 802.11 Update Station QoS | AC → WTP | modifie la politique de QoS sur le WTP pour une station donnée. S’applique aux paquets reçus par le WTP de la station indiquée par l’adresse MAC du message. |
| IEEE 802.11 Update | AC → WTP | définit un nouveau WLAN sur le WTP. |
| IEEE 802.11 WTP QoS | AC → WTP | Configure la qualité de service sur le WTP |
| IEEE 802.11 WTP WLAN Radio Configuration | AC ←→ WTP | Si utilisé par l'AC, configure une radio sur le WTP. Si utilisé par le WTP il sert à transmettre sa configuration à l’AC. |
| IEEE 802.11 WTP Radio Fail Alarm Indication | WTP → AC | envoyé si le WTP détecte une défaillance radio |
| IEEE 802.11 WTP Radio Information | WTP → AC | communique les informations radio de chaque radio IEEE 802.11 dans le WTP. Il doit être présent dans les messages «Discovery Request», «Primary Discovery Request» et «Join Request» pour que l'AC puisse déterminer la liaison IEEE 802.11 spécifique à utiliser. |

Tableau 3: Quelques éléments pour la mise en place de la norme 802.11dans le protocole CAPWAP.

# **A3** **Différentes informations radio couvertes par l’amendement 802.11k**

## A3.1 Informations sous forme de demande/ réponse

**Beacons:** où la station demandeuse veut avoir des informations concernant les différents points d’accès dans la portée de la station demandée, cette dernière exploite les beacons reçus pour donner l’information.

**Frame:** elle fournit des informations sur le trafic circulant sur le canal et le nombre de trames reçues par la station. Aussi pour chaque émetteur, la station peut fournir son adresse et à quel BSSID il appartient, le nombre de trames reçues depuis cet émetteur, et la puissance moyenne de signal de ces trames (RCPI).

**Channel Load:** elle retourne la valeur d’utilisation du canal, telle observée par la station mesureuse.

**Noise histogram:** elle retourne la valeur de sondage de niveau du bruit (virtual carrier sense) du canal lors de non activité de la station (ni émission, ni réception) pour savoir la puissance de bruit des activités provenant d’autres que les stations IEEE 802.11.

**STA statistics:** elle retourne les valeurs concernant le délai moyen d’accès au BSS et les valeurs concernant la station. Les valeurs concernant la station englobent: le nombre de fragments émis et reçus, le nombre de trames émises et reçues, le nombre de trames émises et reçues en multicast, le nombre d’échecs d’émissions, le nombre de retransmissions, le nombre de trames en double, le nombre de succès et d’échecs lors d’émission des RTS, le nombre d’échecs de réception des Acquittements, le nombre de fragments reçus. Aussi les informations concernant le délai moyen d’accès au BSS incluent: le délai moyen d’accès au point d’accès, le délai moyen d’accès pour chaque catégorie, le nombre de stations associées, et l’utilisation du canal.

**Location Configuration Information (LCI):** elle retourne les informations concernant la localisation de la station en termes de longitude, latitude et altitude. Le rapport peut concerner la station demandeuse, ou celui de la station répondeuse.

**Neighbor report:** cette demande est destinée aux points d’accès qui répondent par la liste des points d’accès voisins et leurs informations, qui sont candidats pour le roaming rapide (fast transition) et la transition (service set transition). Cette information permet à la station de gagner de temps lors du roaming.

**Link Measurement:** elle offre l’information sur la qualité instantanée du lien de la station.

**Transmit Stream/ Category Measurement:** elle permet à une station qui implémente la QoS de demander à une station, qui implémente elle aussi la QoS, l’état d’un lien les reliant. Le rapport contient les mesures du coté émetteur du lien. Les conditions de déclenchement des mesures sont incluses dans la demande, et les mesures sont entamées sous forme de rapport dès la satisfaction des conditions requises.

## A3.2 Informations sous forme de demande seule (sans rapport)

**Measurement pause:** elle permet d’inclure un délai entre les demandes qui nécessitent des réponses sur plusieurs trames. Elle permet aussi d’établir une période entre les demandes répétitives.

## A3.3 Informations sous forme de rapport seul (sans demande)

**Measurement Pilot:** c’est une trame d’action transmise périodiquement par les points d’accès à une périodicité plus courte de celles des beacons et contenant un ensemble d’informations contenues dans les beacons et servant pour guider les stations dans leur opération de balayage (scan).

# A4 Différents services et mécanismes offert par l’amendement 802.11v

**BSS Max idle period management:** Il permet à l’AP d’indiquer aux stations la période maximale pendant laquelle elles peuvent ne pas envoyer du trafic tout en restant connectées à l’AP. Dépassant cette période sans envoyer, la station est considérée comme désassociée. Cela permet d’économiser l’énergie et d’optimiser l’utilisation des ressources radio.

**BSS transition management:** il permet d’indiquer aux stations (non AP) a quel AP elles doivent transiter ou bien la liste des AP préférés pour des raisons d’équilibrage de charge (network load balancing).

**Channel usage:** cette information est fournie par l’AP aux stations pour leur permettre de choisir le lien le moins utilisé en mode non infrastructure ou bien en mode lien direct TDLS (tunnelled direct-link setup).

**Colocated interference reporting:** permet d’offrir des informations à la station demandeuse sur l’interférence au voisinage de la station rapporteuse, pour lui permettre d’ordonnancer ses communications.

**Diagnostic reporting:** permet à une station de demander à une autre station (non AP) des informations permettant de diagnostiquer des problèmes liés au réseau, au matériel, à la configuration et à la capacité de la station.

**Directed multicast service (DMS):** permet aux stations non-AP de demander à l’AP de leur adresser des trames destinées au groupe, sous forme de trames individuelles.

**Event reporting:** permet à une station de demander à une autre (non-AP) de lui transmettre des informations sur un événement temps réel. Le message peut concerner:

-la transition, après une opération de changement d’AP (BSS) réussie. Ce message permet de diagnostiquer s’il y a des problèmes liés à la performance de la transition.

-RSNA (Robust security Network Association), ce message permet de connaître le type d’authentification utilisée, ce message permet de diagnostiquer s’il y a des problèmes reliés à la sécurité et à la performance lors de l’authentification.

- WNM (wireless Network Management) log, donc la station rapporteuse envoie son log à celle qui le demande.

- Peer-to-Peer Link, permet d’informer la station demandeuse que le lien est établi.

**FMS (Flexible Multicast Service):** permet à une station (non-AP) de demander de lui envoyer un ensemble de flux adressés pour le groupe avec un intervalle de temps autre que celui mentionné dans le DTIM (delivery traffic indication map). Cela permet à la station de se réveiller selon le nouveau DTIM et d’économiser de l’énergie. Aussi ce mécanisme permet à la station de recevoir un intervalle plus petit que l’ancien DTIM.

**Location services:** Ce service permet aux AP de fournir des informations sur la localisation pour les applications qui ont besoin, tels que les applications de secours. Les stations peuvent aussi fournir cette information en utilisant les trames de demande et de réponse de mesures radio. Aussi, les trames de configuration de localisation avec les réponses associées permettent de définir les paramètres reliés au service de suivi de localisation.

**Multicast diagnostic reporting:** Ce service permet aux stations d’envoyer des informations concernant le trafic multicast reçu, et ce service peut être utilisé par les AP afin de connaître la qualité de trafic multicast reçu par les stations sous son contrôle.

**Multiple BSSID capability:** Ce service permet d’envoyer les informations concernant plusieurs BSSID dans une seule trame beacon ou réponse de sondage (probe response) au lieu d’envoyer plusieurs trames, chacune correspondant à un seul BSSID. Il permet aussi l’indication de la mise en mémoire de plusieurs trames qui concernent plusieurs BSSID, utilisant un seul élément TIM (Trafic Indication Map) en une seule trame beacon.

**Proxy ARP:** Ce service permet à l’AP d’indiquer la non-réception par les stations des trames ARP et en même temps peut être utilisé pour que les stations restent en mode d’économie d’énergie pour une période de temps plus longue.

**QoS traffic capability:** Ce service permet aux stations utilisant le mode QoS d’indiquer aux applications exigeant la génération du trafic correspondant à une certaine catégorie d’utilisateurs que la station peut assurer ce trafic. Une application de voie peut par exemple utiliser ce service pour avoir la probabilité de blocage en se basant sur le nombre de stations pouvant assurer ce service.

**SSID list:** Ce service permet à une station d’envoyer une trame de sondage (probe request) d’un ensemble de SSID (une liste de SSID) à la fois, au lieu de le faire séparément.

**Triggered STA statistics:** Ce service permet à ce qu’une station génère le rapport de statistiques dès que le seuil définit sera atteint.

**TIM broadcast:** ce service permet que les stations reçoivent une indication sur leur trafic individuel mis en mémoire afin de mieux gérer leur mode d’économie d’énergie (wake up time period).

**Timing measurement:** Ce mécanisme permet aux stations de corriger les dérivations ou décalages des horloges, en se basant sur l’information figurant dans les messages des stations qui envoient.

**Traffic filtering service:** Ce service est utilisé au niveau de l’AP et permet de filtrer le trafic de données et de gestion destiné aux stations selon les demandes préalables des stations. Aussi la station concernée par le filtre peut demander d’être informée dans une trame de la présence d’un tel trafic avant sa livraison.

**U-APSD Coexistence:** ce service permet aux stations d’indiquer à l’AP la durée pendant laquelle la station peut recevoir les trames, afin d’éviter les périodes durant lesquelles la station connaît un niveau élevé d’interférence.

**WNM-Notification:** Il permet à une station de notifier une autre d’un événement de gestion tel que la présence d’une mise à jour de la firmware.

**WNM-Sleep mode:** c’est un mécanisme qui permet aux stations (non AP) d’être en mode sleep étendu, qui permet l’économie d’énergie. En effet la station signale à l’AP la durée pendant laquelle elle va rentrer dans ce mode, ce qu’il lui permet d’être associé à l’AP sans envoyer ni recevoir du trafic.

# Glossaire

Ce glossaire répertorie les mots-clés utilisés dans ce rapport, mais aussi ceux aidant à mieux comprendre le fonctionnement des WLAN, et provenant du standard IEEE802.11.

**access point (AP):** c’est la station qui produit l’accès au service du système de distribution pour les autres stations.

**access point (AP) reachability:** un AP est atteignable par une station si les messages de pré-authentification peuvent être échangés entre eux.

**association:** c’est le service qui permet l’accès à la station et donc l’utilisation des services de système de distribution.

**authentication:** c’est le service permettant l’identification de l’appartenance d’une station à un ensemble de stations ayant le droit de s’associer à l’AP (ou une autre station si le mode sans infrastructure est utilisé).

**basic service area (BSA):** c’est la zone contenant les membres d’un même ensemble de service de base (BSS), elle peut aussi contenir les stations d’un autre BSS.

**basic service set (BSS):** ensemble des stations qui sont synchronisées via le service «join».

**distribution system (DS):** c’est le système utilisé pour interconnecter un ensemble de BSS et le réseau local (LAN) pour créer l’ensemble de service étendu (ESS).

**distribution system service (DSS):** c’est l’ensemble de services permettant au MAC de transporter les tuples MAC entre les stations qui ne communiquent pas directement.

**distribution service:** c’est le service qui délivre les tuples de service MAC en utilisant les informations des associations dans le système de distribution.

**integration service:** permet la délivrance des MSDU entre le système de distribution (DS) et le réseau local via le portail.

**extended service area (ESA):** la zone dans la quelle les membres d’un même ESS peuvent communiquer. Elle est égale ou plus large d’une BSA et peut contenir plusieurs BSS qui se chevauchent, ou bien sont disjoints, ou bien aussi les deux cas.

**extended service set (ESS):** un ensemble de BSS qui sont interconnectés, et qui apparaissent comme un seul BSS logique pour les stations qui sont connectées au système.

**basic service set (BSS) transition:** le changement d’une station d’un BSS à un autre dans le même ensemble étendu de service (ESS).

**extended service set (ESS) transition:** c’est le changement d’association par une station depuis le BSS appartenant à un ESS vers un autre BSS appartenant à un autre ESS.

**fast basic service set (BSS) transition:** le changement d’une station d’un BSS à un autre dans le même ensemble étendu de service (ESS) d’une manière qui minimise le temps de perte de connectivité de données entre la station et le système de distribution.

**independent basic service set (IBSS):** c’est l’ensemble de services de base (BSS) qui forme un réseau indépendant, ne contenant pas d’accès au système de distribution.

**mobility domain:** l’ensemble des BSS, dans le même ensemble étendu de service (ESS), qui accepte la transition rapide BSS (Fast BSS) entre eux, et qui sont identifiés par un même identifiant d’ensemble de mobilité (MDID).

**mobility domain identifier (MDID):** c’est un identifiant qui nome un ensemble de mobilité.

**medium access control (MAC) service data unit (MSDU):** c’est l’information délivrée comme unité entre les services MAC des AP.

**medium access control (MAC) protocol data unit (MPDU):** l’unité de données échangée entre deux entités MAC utilisant le service de la couche physique (PHY).

**traffic category (TC):** c’est une étiquette pour les unités MSDU qui ont une priorité utilisateur distincte (UP, user priority), telle que vue par les entités de couches supérieures, par rapport aux autres MSDU fournies sur le même lien. Les catégories de trafic ont un sens uniquement pour les entités MAC qui prennent en charge la qualité de service (QoS) au sein du service de données MAC. Ces entités MAC déterminent la valeur UP pour les MSDU appartenant à une catégorie de trafic particulière en utilisant la valeur de priorité fournie avec ces MSDU au niveau de service MAC des AP (MAC SAP).

**enhanced distributed channel access (EDCA):** c’est le mécanisme d’accès CSMA (accès multiple à détection de collision) prioritisé utilisé par les stations acceptant la qualité de service dans un ensemble de services de base QS (BSS). Ce mécanisme d'accès est également utilisé par le point d'accès QoS (QoS AP) et fonctionne concurremment avec la fonction de coordination hybride (HCF) d'accès au canal contrôlé (HCCA).

**robust security network association (RSNA):** c’estle type d’association utilisé par la station si la procédure d’authentification ou d’association utilisée inclue les 4 étapes de handshake ou le protocole FT (fast transition). L’existance de RSNA entre deux paires n’implique pas une sécurité robuste, puisque cette dernière est assurée si toutes les stations utilisent le RSNA.

**robust security network association (RSNA) capable (RSNA-capable):** si la station est capable de créer RSNA.

**robust security network (RSN):** c’est un réseau sécurisé permettant la création des associations robustes sécurisées (RSNA). Un RSN peut être identifié par l’indication de l’élément RSNE dans les beacons des trames que le chiffrement n’est pas celui de WEP (wired equivalent privacy).

**access category (AC):** Une étiquette pour l'ensemble commun de paramètres d'accès aux canaux distribués améliorés (EDCA) utilisés par une station implémentant la qualité de service afin d’accéder au canal pour transmettre les unités de données de service MAC (MSDU) avec certaines priorités.

**enhanced distributed channel access function (EDCAF):** une fonction logique dans la station implémentant la QoS qui détermine, en utilisant l'accès amélioré au canal distribué (EDCA), le moment où une trame dans la file d'attente de transmission avec la catégorie d'accès associée (AC) peut être transmise via le support sans fil (WM). Il y a un EDCAF par AC.

**fast basic service set (BSS) transition (FT) initial mobility domain association:** la première procédure d’association ou ré-association dans un domaine de mobilité durant laquelle la station indique qu’elle utilise la procédure FT.

# Références bibliographiques

-[1] P. Brenner, “A technical tutorial on the IEEE802.11 protocol,” BreezeCom Wireless Communications, vol. 1, 1997.

-[2] A. Raschella, F. Bouhafs, M. Seyedebrahimi, M. Mackay, and Q. Shi, “Quality of Service Oriented Access Point Selection Framework for Large Wi-Fi Networks,” IEEE Transactions on Network and Service Management, vol. PP, no. 99, pp. 1–1, 2017.

-[3] L. Li, M. Pal, and Y. R. Yang, “Proportional Fairness in Multi-Rate Wireless LANs,” in IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, April 2008.

-[4] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, “Performance anomaly of 802.11b” in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies, vol. 2. IEEE, 2003, pp. 836–843.

-[5] A. Babu and L. Jacob, “Performance analysis of IEEE 802.11 multirate WLANs: time based fairness vs throughput based fairness,” in Wireless Networks, Communications and Mobile Computing, 2005 International Conference on, vol. 1. IEEE, 2005, pp. 203–208.

-[6] F. Kelly, “Charging and rate control for elastic traffic,” European Transactions on Telecommunications, vol. 8, no. 1, pp. 33–37, 1997.

-[7] Y. C. Hsu, K. C. J. Lin, and W. T. Chen, “Client-AP association for multiuser MIMO networks,” in 2015 IEEE International Conference on Communications (ICC), June 2015, pp. 2154–2159.

-[8] I. Koukoutsidis and V. A. Siris, “Access point assignment algorithms in WLANs based on throughput objectives,” in 2008 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, April 2008, pp. 375–383.

-[9]: P. Patras, A. Garcia-Saavedra, D. Malone, and D. J. Leith, “Rigorous and practical proportional-fair allocation for multi-rate Wi-Fi,” Ad Hoc Networks, vol. 36, Part 1, pp. 21–34, 2016.

-[10] M. AMER, A. Busson, and I. Guerin Lassous, “Association Optimization in Wi-Fi Networks: Use of an Access-based Fairness,” in Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, ser. MSWiM ’16. ACM, 2016, pp. 119–126.

-[11] L. H. Yen, T. T. Yeh, and K. H. Chi, “Load Balancing in IEEE 802.11 Networks,” IEEE Internet Computing, vol. 13, no. 1, pp. 56–64, Jan 2009.

-[12] Enterprise Mobility 8.1 Design Guide. Cisco Systems, Inc., 2017.

-[13] O. Brickley, S. Rea, and D. Pesch, “Load balancing for qos enhancement in IEEE802.11e wlans using cell breathing techniques,” in 7th IFIP International Conference on Mobile and Wireless Communications Networks, Maroc, 2005.

-[14] IEEE standard for information technology–local and metropolitan area networks–specific requirements–part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications - amendment 8: Medium access control (mac) quality of service enhancements,” IEEE Std 802.11e-2005. (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003), pp. 1–212, Nov 2005.

-[15] Sanchez, M. Isabel, and Azzedine Boukerche. "On IEEE 802.11 k/r/v amendments: Do they have a real impact?." *IEEE Wireless Communications* 23.1 (2016): 48-55.

-[16] “IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements - part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications,” IEEE Std 802.11- 2016 (Revision of IEEE Std 802.11-2012), pp. 1–3534, Dec 2016.

- [17] S. Govindan, H. Cheng, Z. Yao, W. Zhou, and L. Yang, “Objectives for control and provisioning of wireless access points (CAPWAP),” Tech. Rep., 2006. RFC4564.

-[18] D. Stanley, P. Calhoun, and M. Montemurro, “Control and provisioning of wireless access points (CAPWAP) protocol specification,” 2009. RFC5415

-[19] P. Calhoun, M. Montemurro, and D. Stanley, “Control and provisioning of wireless access points (CAPWAP) protocol binding for IEEE 802.11,” Tech. Rep., 2009. RFC5416

-[20] L. Yang, P. Zerfos, and E. Sadot, “Architecture taxonomy for control and provisioning of wireless access points (CAPWAP),” Tech. Rep., 2005. RFC4118.

-[21] S. Kelly and T. C. Clancy, “Control and provisioning of wireless access points (CAPWAP) threat analysis for IEEE 802.11 deployments,” 2009. RFC5418

- [22] P. Calhoun, “Control and provisioning of wireless access points (CAPWAP) access controller DHCP option,” 2009. RFC5417

-[23] Calhoun, P., O’Hara, B., Suri, R., Cam Winget, N., Kelly, S., Williams, M., and S. Hares, "Lightweight Access Point Protocol", RFC 5412, Feb 2010.

-[24] Modadugu, N., and E. Rescorla. "Datagram transport layer security." (2006). RFC 4347.

-[25] J. Schulz-Zander, L. Suresh, N. Sarrar, A. Feldmann, T. H¨uhn, and R. Merz, “Programmatic Orchestration of WiFi Networks,” in 2014 USENIX Annual Technical Conference (USENIX ATC 14). USENIX Association, 2014, pp. 347–358.

-[26] Gast, Matthew. *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.", 2005.

-[27] M. Liyanage, J. Chirkova, and A. Gurtov, “Access Point Selection Game for Mobile Wireless Users”, International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), Sydney, Australia, 16-19 Jun. 2014.

-[28] K.-L. Hung and B. Bensaou, “Throughput Optimization in Wireless Local Networks with inter-AP Interference via a Joint-association Control, Rate Control, and Contention Resolution,” Ad Hoc Netw., vol. 12, pp. 115–129, Jan. 2014.

-[29] W. Li, Y. Cui, X. Cheng, M. A. Al-Rodhaan, and A. Al-Dhelaan, “Achieving Proportional Fairness via AP Power Control in Multi-Rate WLANs,” IEEE Transactions on Wireless Communications, vol. 10, no. 11, pp. 3784–3792, November 2011.

-[30] A. Baid, M. Schapira, I. Seskar, J. Rexford, and D. Raychaudhuri, “Network cooperation for client-ap association optimization,” in 2012 10th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), May 2012, pp. 431–436.

-[31] L. Chen, “A Distributed Access Point Selection Algorithm Based on No-Regret Learning for Wireless Access Networks,” in 2010 IEEE 71st Vehicular Technology Conference, May 2010, pp. 1–5.

-[32] L. H. Yen, J. J. Li, and C. M. Lin, “Stability and Fairness of AP Selection Games in IEEE 802.11 Access Networks,” IEEE Transactions on Vehicular Technology, vol. 60, no. 3, pp. 1150–1160, March 2011.

-[33] D. Zhao, M. Zhu, and M. Xu, “Leveraging SDN and OpenFlow to Mitigate Interference in Enterprise WLAN.” JOURNAL OF NETWORKS, vol. 9, no. 6, pp. 1526–1533, 2014.

-[34]F. Xu, X. Zhu, C. C. Tan, Q. Li, G. Yan, and J. Wu, “SmartAssoc: Decentralized Access Point Selection Algorithm to Improve Throughput,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, pp. 2482–2491, Dec 2013.