

Chapitre

La technologie IEEE 802.11s Réseaux maillés

1. Introduction

Avec les avancées réalisées dans le domaine des communications sans fil, à la fois au niveau des couches physiques et MAC, le paradigme des réseaux maillés sans fil ou "*Wireless Mesh Network*" a vu le jour. La terminologie réseau maillé sans fil est utilisée pour décrire un ensemble de routeurs sans fil fixes communicant en multi-sauts et qui forment un *backhaul* derrière des point d'accès sans fil qui servent les clients mobiles. Plusieurs technologies sans fil supportent ce type de communication, par exemple, on peut citer IEEE802.11s (WLAN, pour *Wireless Local Area Networks*), IEEE802.15.4 (WPAN, pour *Wireless Personal Area Networks*), et IEEE802.16 (WMAN, pour *Wireless Metropolitan Area Networks*). Dans ce chapitre, nous nous focalisons sur la technologie réseaux maillés à base de l'IEEE 802.11. Le groupe de travail au sein de la famille 802.11 qui est en charge de la standardisation des réseaux maillés est le 802.11s.

Le 802.11s est une évolution des réseaux WLAN 802.11 qui facilite la formation d'un réseau maillé entre des points d'accès 802.11, dans un objectif d'étendre la couverture du réseau WLAN. Un réseau maillé est un réseau multi-saut basé sur une infrastructure contrairement à un réseau ad hoc (MANET pour *Mobile Ad hoc NETWORKS*) [MANET] qui lui ne nécessite aucune infrastructure préexistante. Il offre naturellement un accès sans fil, avec un coût attractif, des débits élevés, et une

2 Les réseaux sans fil émergents

latence contrôlée. Un réseau maillé est interconnecté à l'Internet par un ensemble de passerelles, et le trafic des clients est véhiculé en utilisant un système de communication multi-sauts.

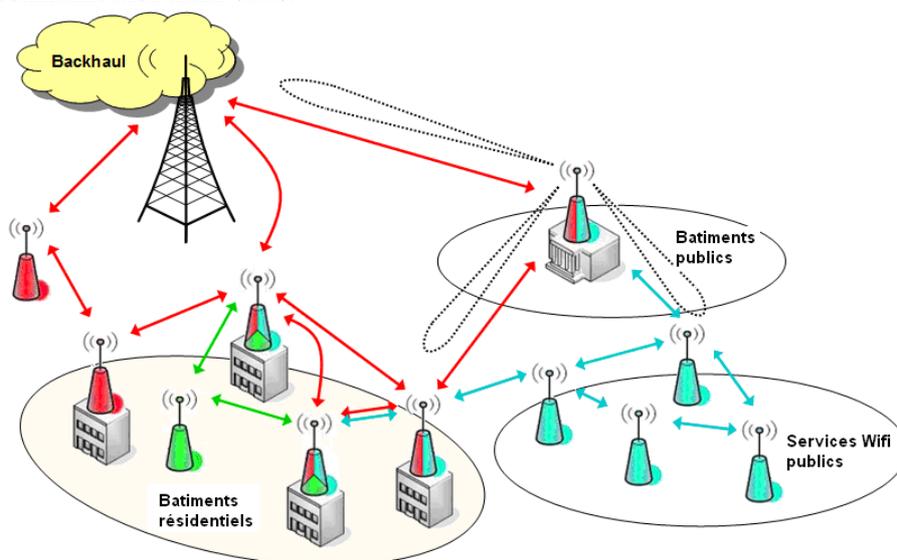


Figure 1. Déploiement métropolitain pour les réseaux maillés.

Plusieurs cas d'usage sont envisageables pour les réseaux maillés. En effet, bien que de telles techniques soient initialement conçues pour étendre la connectivité des réseaux WLAN grâce à une association dynamique des points d'accès, les réseaux maillés peuvent être utilisés pour fournir une connectivité intermittente dans les champs de batailles, ou encore interconnecter des campus universitaires. Ils sont également candidats pour la mise en place des réseaux domestiques ainsi que les réseaux d'entreprises (cf. Figure 1).

Dans ce chapitre nous nous intéressons aux réseaux maillés 802.11s. Le reste du chapitre est organisé comme suit: dans la partie 2 nous rappelons le standard IEEE 802.11. La partie 3 donne une vue d'ensemble du standard IEEE 802.11s. Après une description des cas d'usages des réseaux maillés dans la partie 4, nous détaillons les fonctionnalités et améliorations apportées par le 802.11s dans la partie 5. Avant de conclure, nous décrivons les quelques exemples de déploiement de réseaux maillés à travers le monde dans la partie 6.

2. Le standard IEEE 802.11

Avant de parler du 802.11s, faisons quelques rappels et généralités concernant les différentes topologies qui existent dans le standard 802.11, et qui va nous aider à comprendre l'intérêt et l'apport du groupe 802.11s par rapport aux différentes familles du standard 802.11.

Un réseau 802.11 peut être organisé en deux topologies :

– **BSS (pour *Basic Service Set*)** : un BSS un réseau temporaire (*Short-Lived Network*) formé d'un petit nombre de terminaux. On distingue deux types de BSS :

- *Independent BSS* (IBSS): toutes les stations sont possiblement mobiles. Un réseau ad hoc ou tous les terminaux sont mobiles constitue une *Independent BSS* (cf. Figure 2(a)).
- *Infrastructure BSS*: Au moins un point d'accès est présent dans le BSS. Les réseaux WLAN sont des *Infrastructure BSS* (cf. Figure 2(b)).

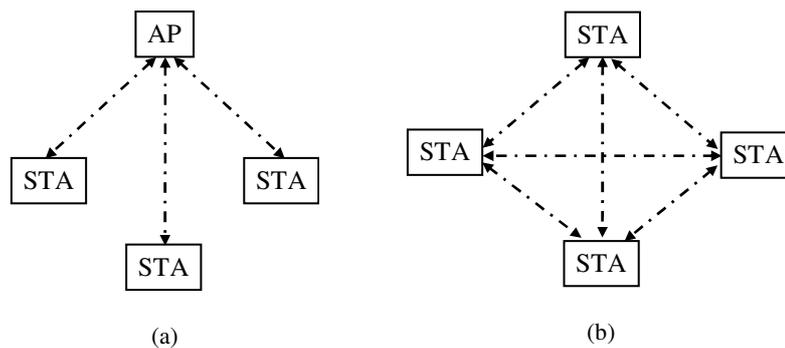


Figure 2. (a) Infrastructure BSS et (b) Independent BSS.

– **ESS (pour *Extended Service Set*)** : un ESS est un ensemble de points d'accès reliés entre eux (ou plus exactement plusieurs BSS) par une liaison appelée système de distribution (noté DS pour *Distribution System*) afin de constituer un ensemble de services étendu (ESS). Le système de distribution (DS) peut être aussi bien un réseau filaire, qu'un réseau sans fil. Les stations peuvent passer de façon transparente d'un point d'accès à un autre.

4 Les réseaux sans fil émergents

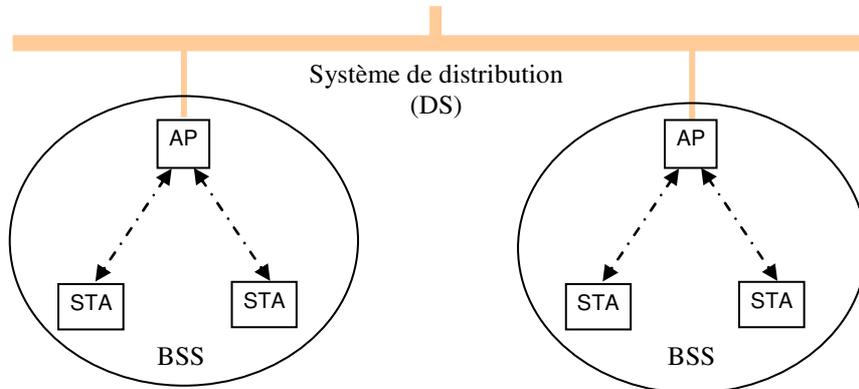


Figure 3. Extended service Set (ESS) dans les réseaux 802.11.

3. Le standard IEEE 802.11s

Le groupe IEEE 802.11s a été créé en Janvier 2004 pour offrir les fonctionnalités du maillage aux architectures et protocoles de la famille IEEE 802.11. Plus spécifiquement, pour définir les amendements nécessaires au niveau des couches MAC et physique pour la création d'un système de distribution sans fil à base de la technologie IEEE 802.11.

Dans les réseaux WLAN non maillés, les stations (STAs) doivent s'associer à un point d'accès (AP) afin d'accéder au réseau, et ces STAs dépendent de ce point d'accès avec lequel ils se sont associés pour communiquer. Dans un réseau maillé les APs peuvent communiquer entre eux directement sans l'intermédiaire d'un réseau externe. Un exemple du modèle WLAN non maillé est illustré dans la Figure 4 et du modèle maillé dans la Figure 5.

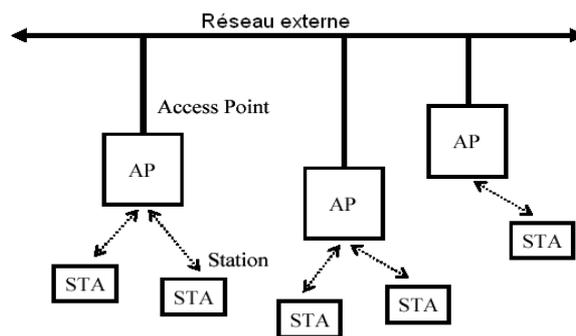


Figure 4. Les communications dans un réseau WLAN classique non maillé.

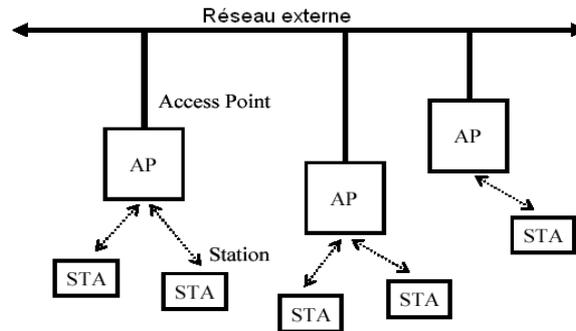


Figure 5. Les communications dans un réseau WLAN maillé.

3.1 Topologie des réseaux 802.11s

La norme IEEE 802.11s [ST2 07] est la norme de l'IEEE 802.11 [ST1 07] pour les réseaux maillés de type ESS. Le groupe de travail associé "s" a été créé par l'IEEE en Juillet 2004. Actuellement le standard est en stade de *draft* c'est-à-dire en cours d'étude non encore standardisé. De manière plus précise, il est à la première *letter ballot* [ST2 07]. L'intérêt porté à ce groupe fait qu'un consensus est difficilement atteignable et fait pousser les échéances. Néanmoins, la norme devrait voir le jour vers 2009.

Un réseau 802.11s est une extension des ESS supportant les communications broadcast/multicast et unicast en mutli-sauts sur une topologie auto-configurable. Le groupe 802.11s travaille principalement sur les points suivants:

- Extension de la technologie 802.11 pour créer un système de distribution sans fil, une gestion automatique des chemins et de la topologie,
- La cible est un réseau de taille moyenne (jusqu'à 32 nœuds dans le cœur du réseau),
- Un protocole de routage avec prise en compte de la qualité des liens,
- Compatibilité avec les couches supérieures.

La norme 802.11s essaye de réutiliser autant que possible les différents mécanismes définis dans les autres normes 802.11, par exemple la sécurité pour le 11i et la QoS pour le 11e. En effet, il est possible d'utiliser n'importe quelle couche physique 802.11 a/b/g/n.

3.2. Terminologie, architecture et découverte de topologie

Un exemple de réseaux maillé est illustré dans la Figure 6. Les nœuds du réseau sont divisés en deux classes : les nœuds possédant des services de maillage, et ceux qui ne les possèdent pas. Nous introduisons ci-après les principaux éléments dans ce type de réseaux :

6 Les réseaux sans fil émergents

- Les stations mobiles (STA) représentent les clients qui consomment le service. Ils ne font pas partie du réseau maillé,

- Point maillé (noté MP pour *Mesh Point*) : tout équipement qui possède les services de maillage, c.a.d. les services de gestion et de fonctionnement du réseau maillé,

- Un point d'accès qui possède les services de maillage sera appelé point d'accès maillé (notée MAP pour *Mesh Access Point*), et c'est le premier point d'accès au réseau maillé. Une telle configuration permet à un équipement de fournir les fonctionnalités d'un point de maillage et de point d'accès simultanément. En comparaison avec MAPs, les MPs participent uniquement aux fonctionnalités de maillage telles que le routage des données,

- Système de distribution sans fil (noté WDS pour *Wireless Distribution System*): c'est la partie sans fil basée sur le 802.11 du système de distribution. Le WDS est formé des MPs qui sont interconnectés entre eux à travers le WDS pour former un WLAN maillé,

- Portail MP (noté MPP pour *Mesh Point Portal*) : joue le rôle de passerelle, et permet d'interconnecter le WLAN maillé à un autre réseau (802.11, ou non). Le MPP et le MAP peuvent être sur un même équipement.

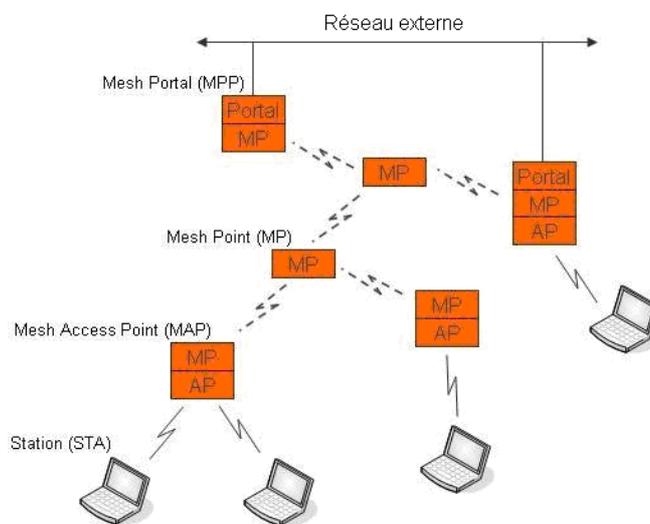


Figure 6. Les équipements 802.11s.

Le 11s se focalise sur les réseaux maillés de troisième génération¹, où on considère le support multi-interfaces et multi-canaux. En effet, on considère que chaque MP peut avoir une ou plusieurs interfaces radio physiques et/ou logiques. Pour ce faire, les MPs doivent être équipés avec plusieurs interfaces 802.11 ou doivent posséder la capacité à changer dynamiquement leur fréquence d'opération. La possibilité d'utiliser plusieurs canaux fréquentiels introduit de la flexibilité au niveau de l'architecture, et permet de l'adapter suivant les besoins et les applications.

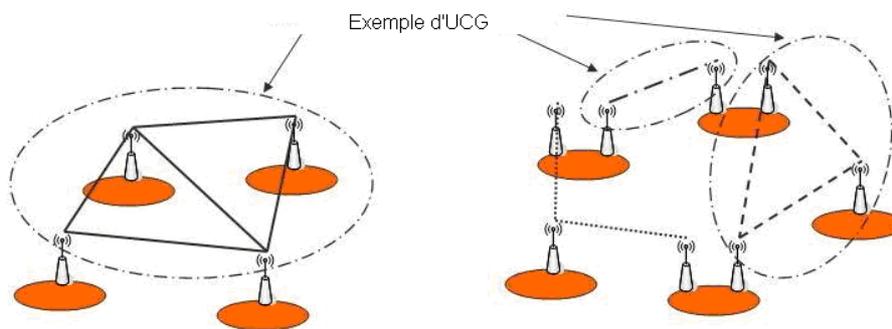


Figure 7. UCG (*Unified Channel Graph*).

Afin d'offrir un maximum de flexibilité dans le déploiement, le 11s propose UCG (pour *Unified Channel Graph*) pour désigner le graphe formé par l'association de l'ensemble des MPs connectés sur un même canal fréquentiel. Cela permettra la mise en place de plusieurs réseaux maillés logiques dans le même réseau physique. Il est à noter également qu'un MP peut appartenir à plusieurs UCGs afin d'interconnecter les différents UCGs

Les MPs qui ne sont pas encore membres du réseau maillé doivent d'abord effectuer une découverte de voisinage pour se connecter au réseau. Pour cela, il utilise un mécanisme de découverte de topologie. Ce dernier peut être passif (écoute des trames balises) ou active (« *Probe Request* » et « *Probe Response* »).

A l'issue de la phase de découverte, un MP va établir des liens avec d'autres MPs (authentification et association), le choix de ces MPs dépend principalement des caractéristiques du lien et de la qualité du signal reçu. Après la phase de découverte, le MP désirant rejoindre le réseau doit être au moins relié à l'un des MPs qui font partie du réseau maillé.

¹ Dans la première génération, le réseau d'accès ainsi que le Backhaul partagent la même technologie radio (802.11b/g). Dans la seconde génération, il ya une technologie radio pour le réseau d'accès (802.11b/g) et une autre technologie radio différente pour le backhaul (802.11a).

4. Les cas d'usages des réseaux maillés

Le 802.11s définit quatre cas d'usages : le résidentiel pour la maison numérique (*digital home*), les entreprises, les lieux publics, et enfin comme infrastructure temporaire en cas de catastrophe. Ces cas d'usage sont détaillés dans ce qui suit.

4.1 Résidentiel

Les réseaux maillés pour le résidentiel, appelé également la maison numérique, permettra de créer à faible coût et avec une facilité de déploiement incomparable une excellente couverture sans fil dans toute la maison. La technologie des réseaux maillés permet d'éliminer les zones non couvertes ou les zones avec une qualité de couverture sans fil médiocre dans toute la maison. Ainsi, les nouvelles applications haut débit comme la transmission et la diffusion de vidéo haute définition (~10Mb/s) seront facilement supportées dans les réseaux domestiques.



Figure 8. Les réseaux maillés pour la maison numérique.

4.2. Entreprise

La motivation principale derrière l'introduction des réseaux maillés pour fournir de la connectivité dans l'entreprise est d'utiliser des technologies sans fil performantes, fiables, peu chers, et faciles à déployer. Les entreprises peuvent ainsi maîtriser les coûts associés à l'installation du réseau et de réduire le temps nécessaire pour le déploiement.

4.3. Zone public (campus, communauté)

Les réseaux maillés sont aussi candidats pour fournir de la connectivité dans les zones publiques. En plus des avantages cités auparavant liés au coût et à la simplicité de déploiement, les réseaux maillés facilitent l'introduction des services de localisation, qui sont d'une importance majeure pour différentes applications. Sur un autre volet, ils participent à l'émergence des réseaux de communauté².

4.4. Réseau temporaire après catastrophe

Les réseaux maillés sont envisageables également pour fournir de la connectivité sans fil pour des pompiers durant leur intervention par exemple, ou pour fournir une infrastructure temporaire pour l'accès à l'Internet après une catastrophe naturelle. Le réseau peut être utilisé pour la vidéosurveillance à distance, la transmission de la voix et des données d'urgence, etc....

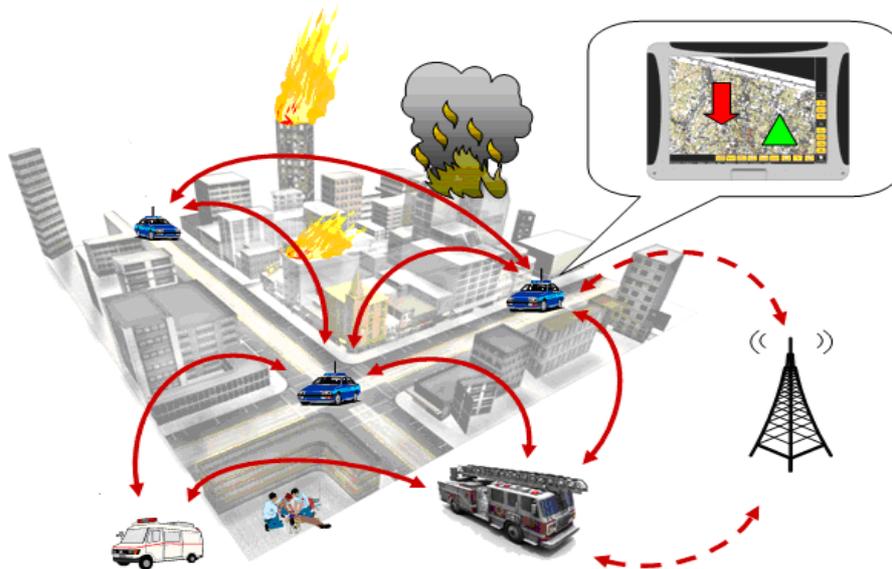


Figure 9. Mise en place d'un réseau maillé après incendie (les nœuds sont considérés comme fixes).

² Un réseau de communauté est un réseau maillé formé exclusivement par un ensemble d'utilisateurs qui coopèrent entre eux pour la réalisation de certaines applications ou services.

5. Fonctionnalités et améliorations apportées par le 802.11s

Dans cette section nous allons donner une vue d'ensemble sur les différentes solutions proposées pour le routage, la sécurité et les optimisations de la couche MAC dans ces réseaux.

5.1. Protocoles de routage

Le routage, aussi appelé sélection de chemin, consiste à trouver la route optimale. Les protocoles de routage 802.11s sont particulièrement basés sur les travaux du groupe IETF MANET [MANET], mais fonctionnent au niveau 2 à la différence des protocoles MANET qui sont eux plutôt de niveau 3. Le groupe 11s a fixé comme configuration cible un réseau qui contient jusqu'à 32 entités qui participent dans le routage. Mais des configurations avec plus de nœuds restent possibles. Deux protocoles de routage sont considérés :

– HWMP (pour *Hybrid Wireless Mesh Protocol*) : c'est le protocole de routage par défaut. Comme son nom l'indique, le protocole HWMP combine deux protocoles de routage avec des modes différents, tous les deux de type vecteur de distance : le premier mode est un routage à la demande RM-AODV (pour *Radio Metric Ad hoc On-Demand Vector*), le deuxième est un routage à base d'arbre (*Tree Based Routing*). Cette combinaison rend le protocole performant suivant que le réseau maillé est connecté à un réseau fixe ou non. Ces deux protocoles sont détaillés ci-après :

- RM-AODV : c'est une variante du protocole AODV (pour *Ad hoc On Demand Distance Vector*) [PER 03]. Il consiste à utiliser un mécanisme de requêtes RREQ (pour *Route REQuest*) et RREP (pour *Route REPLY*). Quand un MP *S* veut connaître la route vers un MP *D*, il envoie en diffusion une requête de demande de route RREQ. Ce message sera rediffusé de proche en proche par les MP intermédiaires (on suppose qu'il existe un mécanisme d'élimination des boucles) jusqu'au MP *D*. Un champ particulier dans ce message indique le coût du chemin traversé du MP *S* jusqu'au MP courant, ce qui permettra de sélectionner le chemin avec le meilleur coût. A la réception de la requête RREQ, le MP *D* renvoie vers *S* un message de réponse RREP. RM-AODV est utilisé pour le routage entre les clients dans le maillage ou ce qu'on appelle *P2P Mesh Routing*.
- Routage à base d'arbre : Ce protocole consiste à configurer un MP particulier comme étant la racine de l'arbre. Le protocole se déroule en deux phases, une première phase de construction d'arbre : la racine diffuse périodiquement un message « *Root Announcements* » avec un champ distance de valeur zéro. Les MPs ensuite rediffusent ce message (aussi

problème de boucles) tout en mettant à jour la distance vers la racine. A la fin de la première phase, chaque MP a choisi un MP père. Ce MP père se situe sur le plus court chemin vers la racine. La deuxième phase consiste à enregistrer les MPs et leurs stations auprès de la racine en envoyant un message « *Gratuitous RREP* ». Maintenant lorsqu'un MP *S* veut envoyer une trame vers un MP *D*, il l'envoie vers la racine qui la relaie vers *D*. Cette stratégie est efficace pour le routage vers les passerelles.

– RA-OLSR (pour *Radio-Aware Optimized Link State Routing*): C'est un protocole de routage optionnel. Il est adapté pour des réseaux avec une faible mobilité (ce qui est le cas dans les 11s). Il est basé sur le protocole de routage OLSR (*Optimized Link State Routing*) [CLA 03] développé par le groupe de travail IETF MANET avec l'utilisation de métriques radios pour les décisions de routage.

La métrique de routage par défaut est le *AirTime* sur chaque lien, et qui correspond à la quantité de ressource radio consommée lors de la transmission d'une trame sur un lien. Elle est calculée selon la formule suivante :

$$C_a = \left[O_{ca} + O_p + \frac{B_t}{r} \right] \frac{1}{1 - e_{pt}} \quad [1]$$

Où r désigne le débit en Mb/s et e_{pt} le taux d'erreur par trame avec l'utilisation d'une trame de longueur B_t . La table ci-dessous donne les valeurs par défaut pour les différents paramètres dans la formule [1] proposée :

Paramètre	Valeur (802.11a)	Valeur (802.11b)	Description
O_{ca}	75ms	335ms	Channel access overhead
O_p	110ms	364ms	Protocol overhead
B_t	8224	8224	Nombre de bit dans la trame de test

Table 1. Valeur des paramètres nécessaires pour le calcul de la métrique *AirTime*.

Néanmoins, l'architecture et les protocoles proposés supportent facilement l'introduction de nouvelles métriques. En effet, les protocoles de routage peuvent utiliser des mesures sur le réseau maillé afin de déterminer la meilleure route. Les mesures utilisées sont : (i) la qualité du lien maillé en termes de délai, Jitter, débit, bruit, SNR (pour *Signal Noise Ratio*), et (ii) la qualité de la route et donc la meilleure route parmi celles possibles (suivant les critères cités dans le premier

point). D'autres mesures définies par le 802.11k [ST3 07] (mesures des ressources radio) peuvent et devraient être utilisées pour le routage dans les réseaux maillés.

Les protocoles de routage doivent supporter l'unicast et également le broadcast/multicast. L'unicast est principalement supporté par les deux algorithmes de routage. Pour le broadcast, des mécanismes d'élimination de boucles de niveau 2 sont proposés par les deux protocoles de routage également. En effet, un mécanisme basé sur les numéros de séquence est utilisé par RM-AODV et un arbre de broadcast optimisé est généré par RA-OLSR. Pour ce qui est du multicast, il est basé sur le mécanisme de broadcast.

Actuellement, les principaux équipementiers de réseaux maillés (Nortel, Cisco, StrixSystems, Mesh Dynamics, Columbris, Proxim, Motorola, etc.) ont développé leur propre protocole de routage en adaptant les protocoles de routage existants tels qu'OSPF (pour *Open Shortest Path First*) ou l'arbre de recouvrement (*Spanning Tree*). La version modifiée de *Spanning Tree* est utilisée au niveau 2, tandis qu'OSPF est utilisé au niveau 3.

5.2. Mécanismes d'amélioration de la couche MAC

En raison du multi-saut, les flux avec un débit équivalent et un nombre de saut différent par rapport à la passerelle (l'élément logique permettant de connecter le réseau 802.11 au réseau filaire) consomment des ressources différentes à cause de cette distance par rapport au portail. Par conséquent, les ressources disponibles doivent être efficacement allouées. Dans cette section, nous allons discuter le mécanisme EDCA (pour *Enhanced Distributed Channel Access*) dans le cadre de la norme 802.11s. Ce mécanisme proposé par le groupe 802.11e (EDCA) [STD 05] est retenu comme le mécanisme par défaut dans la norme 802.11s. D'autres optimisations optionnelles sont également disponibles : MDA (*Mesh Deterministic Access*), *Intra-mesh Congestion Control*, CCF (*Common Channel Framework*), Gestion de l'énergie, la synchronisation [HIE 07] [CAM 08]. Ils sont présentés par la suite.

5.2.1. EDCA (Fonction par défaut)

Pour les liens sans fil, l'amélioration QoS au niveau de la couche MAC introduite par 802.11e [STD 05], appelé EDCA (pour *Enhanced Distributed Channel Access*) ou aussi WMM (pour *WiFi MultiMedia*), est utilisée comme base pour le 802.11s. EDCA propose jusqu'à 4 catégories d'accès: *Voix* (priorité plus élevée), *Vidéo*, *Best effort* (pour le trafic des applications standards) et *Background* (priorité plus basse pour un trafic avec peu d'importance) et améliore DCF (pour *Distributed Coordination Function*) selon trois principes :

– Gestion des files d’attente par les équipements maillés (point d’accès ou station) : chaque équipement gère une file d’attente par classe de trafic. Un paquet à transmettre entre donc dans la file d’attente selon sa classe de trafic.

– Le mécanisme AIFS (pour *Arbitration Inter Frame Space*) est le même que DCF, cependant les messages à haute priorité ont plus de chance d’être émis rapidement que ceux à basse priorité. Pour cela EDCF règle les délais DIFS (pour *Distributed Interframe Space*) et la fenêtre de contention CW (pour *Contention Window*) selon les classes ; plus la classe est prioritaire, plus les délais d’attente sont courts. On ne parle plus de DIFS mais d’IAFS (dont la durée est supérieure ou égale au DIFS).

– TXOP (ou *Transmission Opportunity*) : EDCF permet aussi aux stations d’émettre plusieurs messages successifs (en rafale). La station profite d’une « opportunité de transmission » (TXOP). La durée maximale d’une TXOP peut être précisée dans les trames balises de l’AP. Pendant un TXOP la station émet autant de messages qu’elle le souhaite les uns après les autres en ne les espaçant que de SIFS (pour *Short InterFrame Space*). Puisque SIFS est le délai le plus court que personne ne peut interrompre. Les classes *voix* et *vidéo* peuvent envoyer une série non interrompue de trames en utilisant TXOP. Les autres classes envoient seulement un paquet sans durée limite chaque fois qu’elles obtiennent l’accès au médium sans fil. Il est recommandé d’exiger un contrôle d’admission pour la voix et la vidéo. Ce mécanisme permet de limiter le nombre de flots de trafic utilisant les classes de haute priorité.

EDCA est simple à mettre en œuvre et permet de régler les flux en fonction des classes de trafic. Il augmente la probabilité pour un paquet prioritaire à être envoyé. Cependant, il repose sur le hasard (il peut arriver que certains messages prioritaires soient retardés un peu trop longtemps) et la « famine » (un message peu prioritaire peut être émis avec beaucoup de retard s’il y a un trafic régulier et plus prioritaire sur le réseau) peut faire perdre de l’efficacité au réseau.

5.2.2. MDA (*optimisation optionnelle*)

MDA (pour *Mesh Deterministic Access*) est une méthode d’accès optionnelle qui permet à des MP d’accéder au canal à des instants donnés avec la moindre contention possible. Il est basé sur un protocole de réservation via un simple échange (appelé en anglais "*shackehand*") entre l’émetteur-récepteur pour établir des périodes MDAOPs (pour *MDA Opportunities*). Chaque MP maintient et diffuse dans ses trames balises des informations sur (i) la liste de tout les MDAOPs pendant lesquelles il est soit émetteur soit récepteur, et (ii) la liste des MDAOPs voisines. Ceci permet aux MPs voisins d’éviter des recouvrements entre les réservations MDA. Une fois qu’un MP obtient un MDAOP, il effectue un CCA (pour *Clear Channel Assessment*) et accède au médium avec la plus haute priorité. Les MPs

voisins s'abstiennent d'accéder au canal pendant cette période. La Figure 10 montre le fonctionnement de MDA. Il faut noter que les connexions MDA ne peuvent être mises en place qu'entre des MPs supportant tous le MDA.

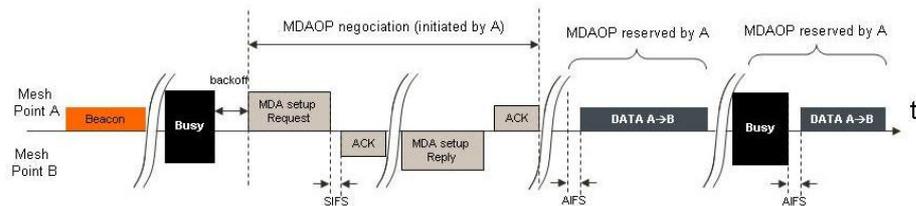


Figure 10. Mécanisme MDA. Le MP *A* négocie un MDAOP avec le MP *B*. Le MDAOP négocié est périodiquement assigné pour envoyer des données à *B*. Si le médium sans fil est occupé au début d'un MDAOP, alors il est réduit. Cependant, MP *A* doit subir le procédé de backoff pour accéder au médium pendant son MDAOP [HIE 07].

5.2.3. Intra-mesh congestion control (optimisation optionnelle)

Le mécanisme de contrôle de congestion Intra-maille est un mécanisme simple de contrôle de congestion implémenté dans chaque nœud. Chaque nœud surveille activement l'utilisation locale du canal. Si la congestion est détectée, le nœud informe les voisins précédents et/ou le voisinage. Chaque nœud qui reçoit un message de congestion soit en unicast soit en broadcast devrait ajuster son débit en conséquence. Le débit local est ajusté selon la catégorie d'accès (par exemple, le taux du trafic *Best effort* doit être ajusté sans affecter le trafic *voix*).

5.2.4. CCF (optimisation optionnelle)

Le mécanisme CCF (pour *Common Channel Framework*) permet la négociation du canal pour l'échange de données entre deux entités. Un canal commun est utilisé avant de passer à un canal destination. Une fois que les données sont échangées, les deux entités passent de nouveau au canal commun.

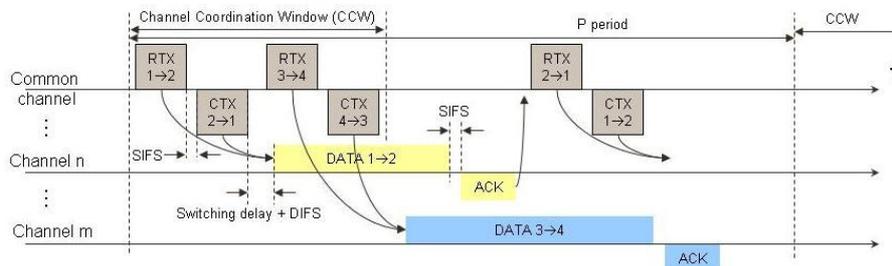


Figure 11. Le mécanisme CCF (RTX: *Request to switch* / CTX: *Clear to switch*).

Comme le montre la figure ci-dessus, une fenêtre CCW (pour *Channel Coordination Window*) pendant laquelle les canaux sont réservés, et une période P pendant laquelle les transmissions utilisent ces canaux réservés, permettent aux nœuds de manipuler périodiquement l'attribution du canal : La fenêtre CCW est définie sur le canal commun et est périodiquement répétée (période P). Les transmissions lancées en utilisant CCF doivent se terminer avant la période P . Le vecteur d'utilisation des canaux (U) de chaque MP est remis à zéro au début de chaque CCW. Un canal réservé pendant le CCW peut être réutilisé par les mêmes entités (nouveau RTX/CTX) au delà de la durée du CCW (avant la fin de la période courante P).

Ce mécanisme peut être utilisé pour des réseaux maillés multi-canaux et unicanaux. Les entités avec des radios multiples peuvent utiliser un canal commun séparé pour chaque interface. Un réseau backhaul utilisant des nœuds avec une seule interface radio doit partager le même canal entre tous les nœuds ; ainsi seulement un couple de nœuds peut communiquer à la fois. Le mécanisme du canal commun alloue temporairement un canal pour les échanges entre deux nœuds et permet ainsi à des nœuds de communiquer deux par deux en même temps.

5.2.5. Mécanismes d'économie d'énergie (optimisation optionnelle)

Tandis que les MAPs doivent rester sans interruption éveillées, les MPs peuvent optionnellement avoir un mécanisme d'économie d'énergie PS (pour *Power Save*) s'ils n'ont pas un raccordement permanent à une source d'énergie. Les dispositifs entièrement chargés peuvent rester éveillés sans interruption pour router plus efficacement le trafic, mais quand le niveau de puissance devient critique, ils doivent passer à un mode sommeil pour conserver leur énergie.

Le mécanisme d'économie d'énergie introduit par la norme 802.11e [STD 05] peut être mis en application pour le réseau d'accès (c.a.d. entre les stations et l'AP). Ce mécanisme s'appelle APSD (pour *Automatic Power Save Delivery*) où les stations comptent sur l'AP pour économiser leurs énergies. Le mécanisme APSD est basé sur des périodes de réveil défini dans la trame balise quand l'AP doit envoyer un paquet à une station. La station se réveille périodiquement et écoute les trames balises. Si elle voit qu'elle a du trafic qu'il lui est destiné, la station se met en mode réveil et génère une trame PS-Poll (pour *Power Save-Poll*) pour demander la livraison du trafic auprès de l'AP.

Le standard 802.11s propose une gestion optionnelle d'économie d'énergie dédiée au lien mesh-à-mesh. Ce mécanisme utilise la gestion d'économie d'énergie définie pour le 802.11 en mode ad hoc IBSS (pour *Independent Basic Service Set*). Il

est basé sur une période de réveil périodique et synchronisé pour chaque entité. Les nœuds gardent dans leurs files le trafic destiné vers un nœud en sommeil. Quand le nœud destination se réveille, les trames en attente lui sont envoyées.

Pour être plus spécifique, un nœud reste réveillé au moins une période ATIM (pour *Announcement Traffic Indication Message*). Pendant cette durée, trois méthodes peuvent être utilisées pour envoyer les trames unicast en attente : (i) le nœud envoie une trame ATIM pour inviter le pair à rester dans l'état éveillé pour davantage de livraison de trames (voir le cas 1 dans la figure suivante), (ii) le nœud utilise l'information TIM (pour *Traffic Indication Map*) incorporé dans la trame balise pour indiquer le trafic bufférisé à son pair. Le nœud pair génère ainsi une trame PS-Poll pour demander la livraison du trafic (voir le cas 2 dans la figure suivante), (iii) le nœud envoie les trames unicast bufférisés pendant l'intervalle ATIM (voir le cas 3 dans la Figure 12).

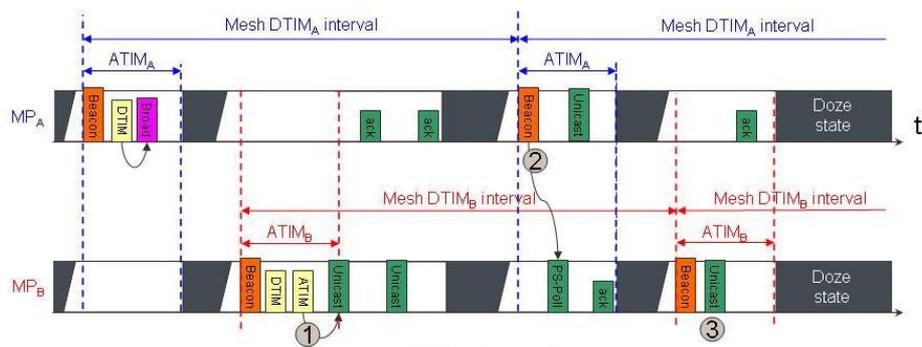


Figure 12. Mécanisme d'économie d'énergie entre deux paires A et B .

Le mécanisme d'économie d'énergie peut être combiné avec le mécanisme CCF. Quand le nœud a des trames bufférisés à envoyer, il peut également proposer un nouveau canal pour échanger les données. Le canal commun est alors utilisé uniquement pour vérifier s'il ya un trafic en suspens et pour recevoir le trafic multicast ou broadcast.

5.2.6. La synchronisation (optimisation optionnelle)

Dans le 802.11s la synchronisation est optionnelle. Beaucoup de services MAC du 802.11s se basent sur la synchronisation : l'économie d'énergie, mécanisme du canal commun, MDA. La synchronisation est aussi nécessaire afin d'éviter la collision des trames de contrôle.

Avec la synchronisation, chaque nœud du réseau maillé met à jour ses horloges suivant les informations (*offset* et *timestamp*) contenues dans les balises réponses reçues de la part des autres nœuds, maintenant ainsi un temps TSF (*Timing Synchronization Function*) commun dans le réseau.

5.3. Sécurité

La sécurité dans le 802.11s se base sur les mécanismes proposés par le standard 802.11i [STD 04]. Le 802.11i, ratifié le 24 juin 2004, fournit une solution de sécurisation des réseaux 802.11. Il intègre les mécanismes déjà utilisés du 802.1x et du WPA. La seule différence notable est la disparition du WPA 1 (RC4) au profit du WPA 2 (AES pour *Advanced Encryption Standard*), beaucoup plus sûr. Contrairement au WPA 1, le WPA 2 permet de sécuriser aussi bien les réseaux sans fil en mode infrastructure que les réseaux en mode ad hoc. La norme IEEE 802.11i définit deux modes de fonctionnement :

- Authentification distribuée (ou WPA Personnel) : le mode WPA personnel permet de mettre en œuvre une infrastructure sécurisée basée sur le WPA sans mettre en œuvre de serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelée PSK (pour *Pre-shared Key*), renseignée dans le point d'accès ainsi que dans les postes clients. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le WPA permet de saisir une phrase secrète (*passphrase*), traduite en PSK par un algorithme de hachage.

- Authentification centralisée (ou WPA Enterprise) : le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS (pour *Remote Authentication Dial-in User Service*), et d'un contrôleur réseau (le point d'accès)

Notons que le 802.11i propose la sécurité d'un lien Wifi. Cependant, une sécurité de bout en bout (e2e) peut être assurée à une couche plus haute.

Les fonctionnalités spécifiques développées par le groupe 802.11s sont :

- Authentification mutuelle entre les nœuds maillés. En effet, quand un nouveau nœud maillé MP découvre un MP candidat, il effectue une première authentification MSA (pour *Mesh Security Association*) avec un MA (pour *Mesh Authenticator*) dans le réseau. Une fois que le nœud maillé fait partie du réseau maillé, il a ainsi les clefs nécessaires pour s'authentifier avec d'autres MP candidats.

- Protection des messages de gestion et de contrôle échangés entre les nœuds maillés (par exemple les informations de routage et de topologie).

5.4. Interconnexion avec les réseaux externes (Interworking)

Comme décrit précédemment, un réseau maillé est utilisé principalement pour étendre la connectivité d'un réseau filaire par l'association en multi-saut de plusieurs MP. L'objectif de l'interworking est d'assurer la transmission de paquets qui sont émis d'un réseau externe vers un client dans le réseau maillé, ou bien vers une autre machine se trouvant dans un autre réseau et transportés via le réseau maillé. Cette problématique est clairement présentée dans la Figure 13 où un réseau maillé est interconnecté à plusieurs réseaux filaires.

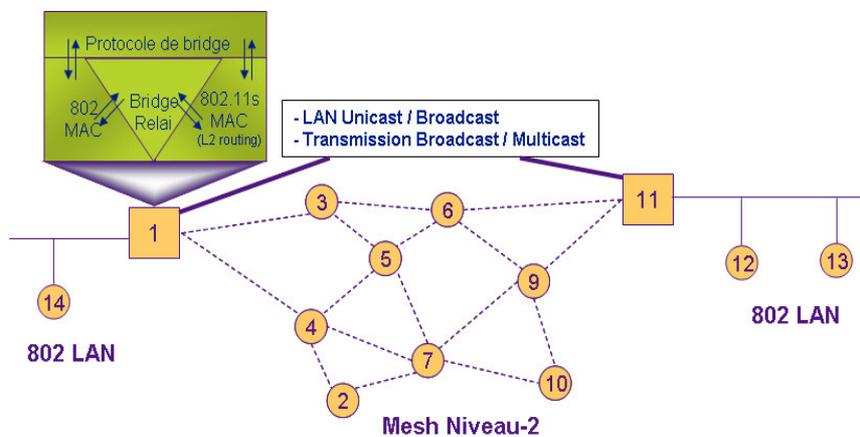


Figure 13. Interconnexion d'un réseau maillé avec des réseaux externes.

Les MPPs relient les réseaux filaires et sans fil. Pour la couche 2, les MPPs utilisent le standard IEEE 802.1d, et pour la couche 3, le routage doit être effectué de la même façon que pour les routeurs IP. Ainsi, pour livrer un paquet, un MP détermine si la destination est à l'intérieur ou à l'extérieur du réseau maillé, en utilisant une découverte de chemin de niveau 2. Pour une destination à l'intérieur du réseau maillé, le MP utilise une découverte de route de niveau 2. Pour une destination en dehors du réseau maillé, le MP identifie la passerelle MPP cible, et livre les paquets en unicast. Si aucune passerelle cible ne peut être identifiée, les paquets sont livrés à toutes les passerelles du réseau maillé. La Figure 14 illustre en détails les différentes configurations possibles.

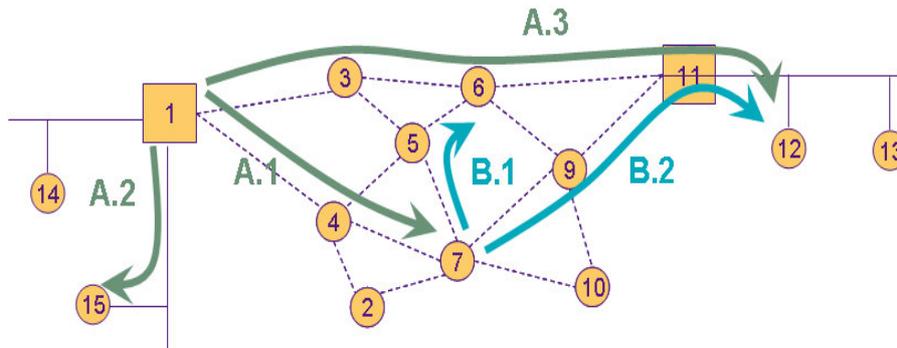


Figure 14. Différentes configurations pour le routage avec interconnexion.

6. Déploiement des réseaux maillés

Dans cette section nous allons décrire quelques exemples de déploiement de réseaux maillés à travers le monde.

– Bruxelles : *Meru Networks* a déployé un réseau maillé de la dernière génération à l'Université libre de Bruxelles (ULB). Il s'agit du réseau maillé le plus important de Belgique. Le réseau maillé est principalement utilisé pour offrir un accès Internet haut débit sécurisé à toutes les personnes qui sont sur le campus universitaire. Des services multimédias comme la voix sur IP et la vidéo seront également fournis à l'ensemble du personnel de l'ULB.

– Nantes : Très récemment, la communauté urbaine de Nantes a annoncé son intention de mettre en place un réseau maillé constitué de 100 point d'accès à travers toute la ville, ce qui fera de lui probablement un des grands réseaux maillés de France. L'opération sera réalisée conjointement par Alcatel-Lucent et SFR. Ainsi, les 200 hectares du centre-ville devraient être couverts en 2008. Le réseau assurera entre autre une continuité de service dans tout le centre-ville. Le réseau maillé devra fournir un débit moyen autour de 5 Mb/s.

– Moscow : *Golden Telecom*, déjà présent dans d'autres grandes villes Russes ainsi que les pays voisins, a déployé un réseau maillé dans toute la ville de Moscow dans le cadre de son partenariat avec *Nortel Networks*. Le réseau maillé composé de 5000 point d'accès *Nortel*, permettra à *Golden Telecom* d'étendre ses services à 3.9 million d'habitants dans Moscow. Des services comme la VoIP, l'accès haut débit ainsi que des services à base de la localisation feront partie du package de connexion.

7. Conclusion

Ce chapitre a présenté un aperçu général sur le standard 802.11s qui a comme objectif d'introduire les fonctionnalités nécessaires dans le standard 802.11 pour supporter les architectures et les protocoles multi-saut maillés.

Les réseaux maillés représentent une technologie prometteuse en pleine essor permettant d'étendre rapidement et facilement la couverture d'un réseau WLAN classique. Ils permettent également la mise en place de solutions abordables et économiquement viables en comparaison aux réseaux filaires pour ramener de la connectivité dans les zones où le coût du câblage est élevé ou impossible. Les pays en cours de développement seront certainement intéressés par une telle technologie qui permettra de combler la fracture numérique entre pays développés et ceux qui sont en voie de développement.

7. Bibliographie

- [CAM 08] J. Camp and E. Knightly, "The IEEE 802.11s Extended Service Set Mesh Networking Standard," *to appear in IEEE Communications Magazine*.
- [CLA 03] T. Clausen, and P. Jacquet, "Optimized Link State Routing Protocol", IETF Internet Std. 3626, October 2003.
- [HIE 07] G. R. Hiertz, S. Max, R. Zhao, D. Denteneer, L. Berlemann, "Principles of IEEE 802.11s," IEEE ICCCN'2007, Honolulu, Hawaii, USA, 13-16 August 2007.
- [MANET] "Mobile Ad-hoc Networks (MANET) Working Group," Internet Engineering Task Force (IETF), <http://www.ietf.org/html.charters/manet-charter.html>.
- [PER 03] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF Internet Std. 3561, July 2003.
- [ST1 07] Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications, IEEE Unapproved draft P802.11-REVma/D9.0, Rev. of IEEE Std 802.11-1999, Mar. 2007.
- [ST2 07] Draft Standard for Information Technology - Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh Networking, IEEE Unapproved draft P802.11s/D1.06, Jul. 2007.

- [ST3 07] Radio Resource Measurement, Draft Amendment to Standard for Information Technology – Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications,” IEEE 802.11k/D7.0, January 2007.
- [STD 05] IEEE 802.11 WG, Draft Supplement to standard for Telecommunications and Information Exchange Between Systems - LAN/MAN Specific Requirements - Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Medium Access Control (MAC) Enhancements for Quality of Service (QoS), IEEE 802.11e/D13.0, Jul. 2005.
- [STD 04] Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE P802.11i/D10.0, April, 2004.

Table des matières

1. INTRODUCTION.....	1
2. LE STANDARD IEEE 802.11.....	3
3. LE STANDARD IEEE 802.11S	4
3.1 TOPOLOGIE DES RESEAUX 802.11s	5
3.2. TERMINOLOGIE, ARCHITECTURE ET DECOUVERTE DE TOPOLOGIE	5
4. LES CAS D'USAGES DES RESEAUX MAILLES	8
4.1 RESIDENTIEL	8
4.2. ENTREPRISE	8
4.3. ZONE PUBLIC (CAMPUS, COMMUNAUTE)	9
4.4. RESEAU TEMPORAIRE APRES CATASTROPHE.....	9
5. FONCTIONNALITES ET AMELIORATIONS APPORTEES PAR LE 802.11S	10
5.1. PROTOCOLES DE ROUTAGE	10
5.2. MECANISMES D'AMELIORATION DE LA COUCHE MAC	12
5.3. SECURITE	17
5.4. INTERCONNEXION AVEC LES RESEAUX EXTERNES (INTERWORKING).....	18
6. DEPLOIEMENT DES RESEAUX MAILLES.....	19
7. CONCLUSION	20
7. BIBLIOGRAPHIE.....	20

Index

MANET 1, 10, 11

Point d'accès 1, 4, 6

Backhaul 1, 2, 15

BSS, IBSS, ESS 3

MP, MPP, MAP 6

Multiinterfaces, multicanaux 7, 15

WLAN 1, 4, 5

Routage 5, 10-12

EDCA, 802.11e 12-13

Sécurité 5, 17