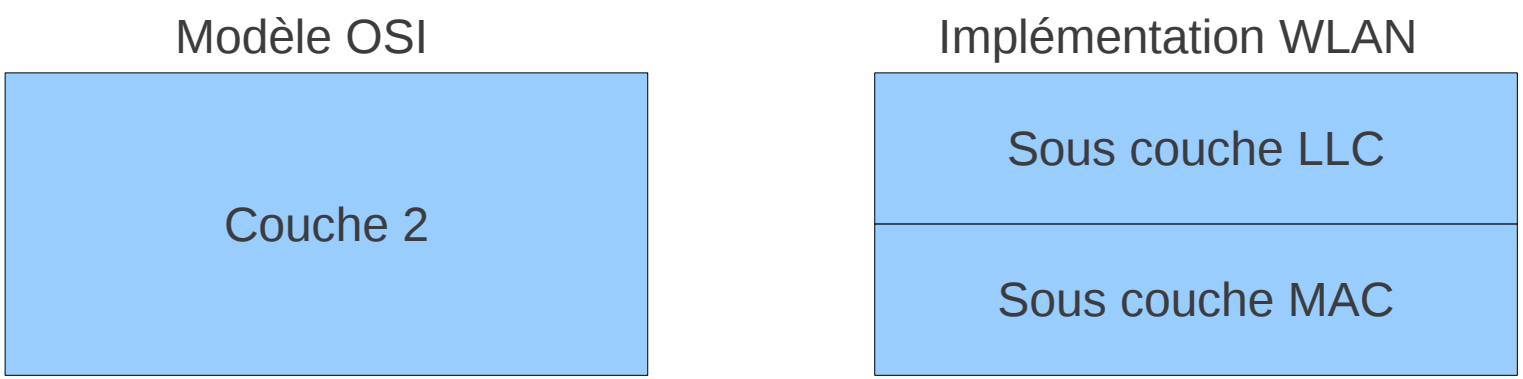
Wireless Local Area Network (Wireless Fidelity)

Ces dernières années ont vu l'essor des réseaux locaux sans fil. Ces derniers inter-opèrent avec les LAN et sont simples d'utilisation. Cependant les difficultés sont nombreuses.

OSI et WIFI

La couche 2 OSI se découpe en 2 sous couches pour les WLAN, comme pour Ethernet.
La sous couche LLC étant commune aux 2 infrastructures.



Fonctionnalités assurées par la sous couche MAC

Elle gère le format des trames MAC et leur fragmentation afin d'assurer une meilleure fiabilité.

Elle gère les fonctions d'économie d'énergie.

Elle assure la connectivité et le partage/accès du/au support.

Accès au support

Il existe 2 méthodes d'accès au support :

- Distributed Coordination Function ou chaque station a accès au support
- Point Coordination Function, le point d'accès gère la coordination de l'accès au support.

Trame de niveau MAC

- Elles sont de 3 types :
  - De données
  - De contrôle pour l'accès au support
  - De gestion pour l'association, l'authentification et la synchronisation
- Toutes ces trames encapsule une trame de base MAC

Format de trames

Trame MAC de base (PLCP Service Data Unit)

champs	contrôle	durée	@1	@2	@3	contrôle	@4	message	checksum
octets	2	2	6	6	6	2	6	0 à Max 2312	

Trames MAC (PLCP Protocol Data Unit)

champs	sync	début trame	PLW	débit	checksum	trame MAC (PSDU)
octets	10	16	12	4	16	

sync est utilisé pour choisir l'antenne
PLW (PSDU lengh Word)

DCF

Ce mode repose sur un mécanisme CSMA avec une fonction Collision Avoidance. En effet dans les transmission hertziennes il n'est pas possible de détecter une collision. Le CSMA/CA tient compte de cette particularité afin de garantir les débits du réseau.

CSMA/CA

Une station écoute le support avant d'émettre. Si le support est libre, elle attend un certain temps (aléatoire) avant d'initier le processus d'émission :
- elle réserve un temps de parole (trame Request to Send)
- elle attend la réponse (trame Clear to Send)
- elle émet
- elle attend un accusé de réception sinon elle réémettra.

PCF

Cette fonctionnalité est ajouté au DCF. La gestion des communications est faite par un point d'accès. Toutes les communications passent par le point d'accès qui les retransmet ensuite. Chaque station se voit attribué un temps d'émission à tour de rôle.

Connexion à un AP

- Il faut 3 étapes :
  - Sondage
  - Authentification
  - Association

Sondage

- La station émet une requête de découverte des AP
  - Service Set IDentifier identifie un réseau
- Elle reçoit une/des réponses
- Elle fait le choix d'une station (suivant un ou des paramètres configurables)

Authentification

- Par adresse MAC (non normalisé)
- Open System
  - Accepte toutes les requêtes
  - Configuration possible sans clé WEP
- Shared key (utilisation de clé WEP), test du chiffrement (4 messages)
- Échange initié par la station

Association

- Permet à un AP d'associer un port à une station
- Échange initié par la station
- 2 messages

Le mode économie d'énergie

- Afin d'assurer une meilleure gestion de l'énergie des stations du WLAN (souvent mobile), il existe un mode économie d'énergie
- Le fonctionnement du mode Power Save est différent pour la communication unicast et les autres.
- En unicast c'est la station qui définie son intervalle d'écoute alors que dans les autres cas, c'est l'AP qui fixe se délai.

Les topologies de WLAN

Elles sont au nombre de 3 :

- Independant Basic Service Set (mode ad-hoc), chaque station communique directement avec les autres
- Basic Service Set, chaque station communique seulement avec un point d'accès (Access Point) qui acheminent ensuite les messages à leurs destinataires
- Extended Service Set, composé de plusieurs BSS reliés entre eux (par câble ou sans fil) via un système de distribution (Distribution System)

Sécurité et Wifi

- Il existe différents moyens de sécuriser un réseau WIFI
- Le chiffrement WEP
- Mécanisme WPA
- Dissimulation du SSID
- Authentification par adresse MAC
- Utilisation de ACL

Authentification par adresse MAC

- Permet de limiter l'accès au réseau
- Peut être contournée par l'utilisation de carte réseau 802.11 où l'on peut changer l'adresse MAC Universelle par une locale

Wired Equivalent Privacy

- Chiffrement par flot RC4
- Clé de 40 ou 104 bits définies statiquement
- Plus une Vecteur d'Initialisation de 24 bits
- Peu consommateur de ressource
- La clé + le vecteur donne grâce à un générateur une séquence d'octet utilisé pour chiffrer le message (OU exclusif)
- Le message chiffré + l'IV sont envoyés

Wifi Protected Access

- Version 2 normalisé par 802.11i, qui définit un Robust Security Network
- Authentification :
  - 802.1x
    - Basé sur le protocole Extensible Authentication Protocol
    - Utilise un serveur d'authentification (Remote Authentification Dial-In User Server)
  - Pre-Shared Key

WPA2

- Chiffrement des données :
  - Temporal Key Integrity Protocol
  - CTR with CBC-MAC Protocol
- Vérification de l'intégrité des données (Message Integrity Check)
- Gestion des clés
- Chiffrement Advanced Encryption Standard

Le matériel WIFI

- Access Point
  - Pour usage domestique (modem, routeur, DHCP, NAT) les box internet
  - Pour un usage d'entreprise (routeur, DHCP, NAT), les Access Point. Gestion du handover
  - Hotspot, permettre une configuration dynamique des paramètres réseaux et un réacheminement SMTP

Matériel

- Contrôleur
  - Gestion du nomadisme et du handover
  - Gestion des points d'accès (puissance, fréquence)
  - Gestion de la sécurité

Matériel

- Les antennes sont de 3 types :
  - Omnidirectionnelle
  - Directionnelle
  - Parabolique
  - Interne
  - Directive (pont)

Matériels

- Les répéteurs permettent de relayer un signal et d'augmenter la taille du réseau.
- Peuvent être sans fil ou filaire

Ponts wifi

- Permettent de créer des ponts entre différents bâtiments de manière à étendre le réseau simplement et facilement.
- Utilisation d'une antenne spécifique

- Au niveau domestique, connecter un équipement au réseau WIFI et Internet

Handover

Capacité/fonctionnalité d'un terminal à changer de point d'accès. Le handover se fait entre 2 transmissions de données contrairement à la téléphonie mobile ou le handover se fait durant la conversation. Les raisons du handover peuvent être diverses :

- mobilité de la station (roaming/itinérance)
- mauvaise qualité de service
- surcharge du point d'accès

Handover, principe

Dans le protocole 802.11, le handover implique une déconnexion avant une reconnexion. Ceci permet d'éviter les boucles et les inondations de messages ainsi que l'utilisation d'un émetteur/récepteur simple.

Notion de domaine

Le handover permet de passer d'un point d'accès à un autre. Lorsque les 2 APs sont situés dans le même ESS (le même domaine), le handover permet de maintenir les sessions applicatives. Ceci n'est pas le cas dans le cas d'un handover entre 2 domaines (ou sous-réseaux) où l'adresse réseau de la station change. IP mobile permet de contrer ces problèmes.

Déroulement du handover intra-domaine

- Détection du besoin de faire un handover
- Recherche du nouvel AP
- Changement d'AP

Détection

- N'est pas spécifier par 802.11
- Implémentation par chaque constructeur
- Les critères sont généralement :
  - Puissance du signal
  - Niveau de retransmission
  - Trames perdues
  - …
- Éviter les handover intempestif

Recherche

- Il existe 2 méthodes pour rechercher un AP :
  - Par balayage actif, la station envoie une requête de recherche (plus rapide mais plus couteux)
  - Par balayage passif, la station analyse les trames balises sur tous les canaux (moins faible, certains réseaux protège leurs données)
- Elle se fait de 2 manières possibles :
  - Avant le handover
  - Pendant le handover

Avant le handover

- Permet de réduire la durée du handover (durée déterminante pour certaines applications)
- Interdit l'envoie et la réception de données pendant cette recherche.
- Est possible pendant le mode économie d'énergie.
- Difficile lors de déplacement rapide

Pendant le handover

- Allonge la durée du handover
- Réduit les interférences avec l'activité de la station

Changement d'AP

- La station initie la ré-association avec le nouvel AP grâce à des trames de ré-association
- Ce changement d'AP induit de nombreuses tâches :
  - Stockage des données sur l'ancien AP
  - Signalisation du nouvel AP auprès de l'ancien
  - Échange du contenu du tampon
  - Mise à jour des tables MAC

Handover inter-Domaine

- Lorsque la station se reconnecte à un nouvel AP qui n'est pas sur le même domaine que l'ancien AP, il s'ensuit un mécanisme de « handover » de niveau supérieur (couche 3). Ceci implique une fin des sessions ouvertes.
- IP mobile permet de limiter les handover de niveau 3

Handover et IP Mobile

- Rappel d'IP Mobile :
  - La station
  - L'agent home (HA)
  - L'agent étranger (FA)

Principe

- Dès que la station a fait son handover, elle initie un handover de niveau IP (voir cours couche réseau)