Les réseaux sans fil

Projet de semestre

Jérémie ANZEVUI
Université de Genève • 2006-2007

SOMMAIRE

INTRODUCTION

“Alors qu'environ 200 millions de puces WiFi ont été vendues dans le monde en 2006, l'institut ABI Research estime dans une récente étude que la barre du milliard d'unités vendues par les différentes industries amenées à utiliser la technologie WiFi devrait être franchie d'ici la fin 2008. Il va même jusqu'à prédire que les livraisons annuelles de puces WiFi dépasseront le milliard de pièces d'ici 2012 grâce à la démocratisation de cette technologie dans les téléphones mobiles et les appareils électroniques grand public, qui compteront tous deux pour deux tiers du marché global du WiFi.

À l'heure actuelle, environ 500 millions de puces WiFi auraient déjà été commercialisées dans le monde depuis l'essor de cette technologie, à laquelle la plateforme pour ordinateurs portables Centrino d'Intel n'est, de l'avis général, pas étrangère. L'arrivée prochaine de la norme 802.11n, qui standardisera l'utilisation de la technologie MIMO (Multiple In, Multiple Out) devrait sans doute contribuer à faire progresser les ventes. En effet, le WiFi 802.11g et ses 54 Mbps montrent aujourd'hui leurs limites dans le cadre d'une utilisation domestique, où la vidéo, les flux de télévision par ADSL et la haute définition requièrent une bande passante de plus en plus importante.”

Clubic.com[1] , 13 février 2007

Pratiquement inconnu, il y a encore quelques années, les réseaux sans fil (WLAN ou Wi-Fi™)[2] sont, aujourd’hui, omniprésents dans notre société. Utilisant des ondes radio, les WLAN existent pourtant depuis des années, mais l’augmentation de la bande passante et la baisse des coûts a fait exploser leurs croissances. Il faut savoir que les premiers WLAN, comme Aloha, ARDIS et Ricochet, offraient des débits inférieurs à 1Mbit/s. Puis vint le standard 802.11 ratifié en 1997. Celui-ci permis alors un d’atteindre un débit compatible entre fabricants de 2Mbit/s. En 1999, on atteint la vitesse de 11Mbit/s grâce au standard 802.11b. Les 54Mbit/s ont été franchis, en 2003, avec le standard 802.11g. En attendant le standard 802.11n, prévu pour 2007, qui permettrait d’atteindre les 600 Mbit/s, un brouillon (“Draft-N”) a été ratifié début 2006 qui permet un débit théorique de 300 Mbit/s soit trois fois plus qu’un réseau Fast Ethernet filaire dont le débit est de 100 Mbit/s.

1 Source: http://www.clubic.com/actualite-69679-puces-wifi-circulation-2008.html

2 cf. glossaire

Les industries ont été les premières à utiliser les WLAN. Ce qui a eu comme effet d'exposer les atouts des communications sans fil dont les coûts étaient encore importants, il y a de ça quelques années. La vente de matériels nécessaire aux WLAN ayant augmenté, les coûts ont fortement baissé rendant accessible cette technologie au grand public.

Les réseaux WLAN au standard 802.11 ont une topologie LAN, mais présentent de nombreuses différences dues à leur technologie. Plusieurs nouveaux points sont à prendre en considération lors de l'installation d'un WLAN, tels que l'étude du site (zone à couvrir), la qualité de service (QoS), la sécurité (qui à accès au réseau ?) et la mobilité des équipements réseau.

Ce projet parcourt les notions fondamentales qui permettent comprendre comment fonctionnent ces WLAN. J'y aborderai ses avantages et ses inconvénients.

LES RÉSEAUX CÂBLÉS

Pour bien comprendre la technologie utilisée par les réseaux sans fil, je commencerai par aborder quelques notions essentielles des réseaux locaux câblés appelés Ethernet.

La plupart des réseaux utilisent une structure hiérarchique composée de trois niveaux. Le paragraphe suivant, tiré du livre "Réseaux WiFi: notions fondamentales" (cf. Bibliographie), les présente:

"

- ***Accès.*** *Assure la connectivité des stations de travail avec le réseau.*
- ***Distribution.*** *Segmente le réseau en domaines de broadcast[3] de niveau 2 par l'emploi de routeur ou de commutateur de niveau 3. Les services réseau, tels que les listes de contrôle d'accès, ou ACL (Acces Control List), le filtrage de routes et la traduction NAT (Network Address Translation), sont appliqués à ce niveau.*
- ***Dorsale (ou backbone).*** *Achemine les trames[2] aussi rapidement que possible entre les niveaux de distributions. Aucun service réseau n'est habituellement impliqué ici. La raison à cela est que la plupart des services nécessitent un traitement des trames ou paquets, qui ralentit le débit. Ce niveau peut être linéaire (couche 2 uniquement) ou hiérarchique (nécessitant un adressage de couche 3).*"

Ethernet 802.3

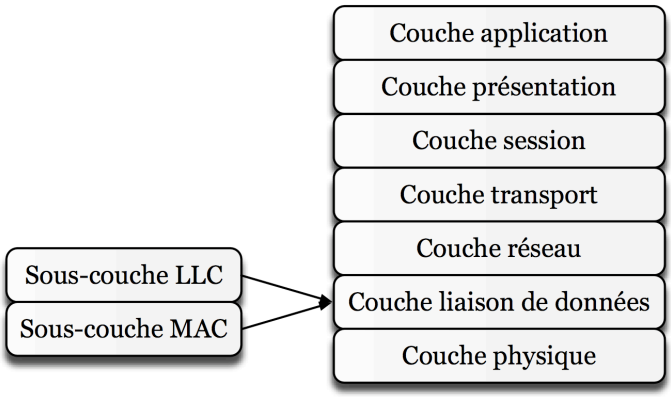
Dans ce chapitre, je vais me focaliser sur le niveau de l'accès et passer en revue les standards 802.3.

Ethernet 802.3 est un protocole réseau permettant la communication de toutes les machines d'un réseau local par une même ligne de communication. Il appartient donc au niveau deux du modèle d'interconnexion des systèmes ouverts (ou OSI en anglais pour *Open Systems Interconnexion*). Ce niveau s'ap-

3,2 cf. glossaire

pelle “couche de liaison de données”. Il est composé des deux sous-couches suivantes:

- **MAC (Medium Acces Control).**
- **LCC (Logical Link Control).**



Modèle de référence OSI

La sous-couche MAC contrôle l’accès au support physique et gère les implémentations spécifiques d’une topologie.

La sous-couche LCC fourni un protocole simple de livraison de trame en mode sans connexion. La principale caractéristique est qu’elle n’offre aucun moyen permettant à l’émetteur de savoir si la trame a bien été reçue.

Les trames Ethernet

Voyons maintenant le format des trames Ethernet 802.3. Elles se composent de sept champs différents:

- **Le préambule.** Long de sept octets (un octet comporte 8 bits), il permet d’indiquer à la station réceptrice qu’une trame est en cours de transmission sur le support.
- **Le SFD (Start of Frame Delimiter).** Long de 8 bits, ce champ indique au récepteur que le contenu de la trame suit immédiatement.
- **L’adresse de destination.** Long de six octets, ce champ représente l’adresse de la station à laquelle la trame est destinée.
- **L’adresse source.** De la même longueur que l’adresse de destination, ce champ représente l’adresse de la station qui émet la trame.
- **Le TLV (Type/Length Value).** Long de deux octets, ce champ identifie le type de protocole de couche supérieure qui est encapsulé dans le champ de données ou de charge utile. La valeur qu’il contient est qualifiée *Ethertype*.

- **Les données ou charge utile.** Ici sont représentés des paquets de niveaux supérieurs. Ce champ a une taille minimale de 46 octets et maximale de 1500 octets (1,5 Ko). Une taille minimale est requise afin que toutes les stations aient une chance de recevoir la trame. Nous ne détaillerons pas ce sujet, mais une recherche Internet avec les mots “diamètre de réseau” ou “timeslot Ethernet” permet d’avoir des éléments de réponses. Au besoin, la station émettrice complète le champ avec des bits de remplissage.
- **Le FCS (Frame Chek Sequence).** Ce champ contient une valeur permettant de contrôler si la trame a été correctement envoyée (la valeur est calculée à partir de la séquence de bit de la trame et est comparée à l’arrivée par la station réceptrice).

L’adressage Ethernet

Longue de 48 bits, une adresse Ethernet est une valeur qui identifie de façon unique une station Ethernet sur un réseau local. Elle est composée de deux parties: un identifiant de 24 bits (assigné par l’IEEE, *Insitute of Electrical and Electronics Engineers*, au fabricant) et un identifiant assigné par le fabricant du matériel. Étant donné que cet adressage renvoie à une interface physique, on parle également d’adresse MAC. Ces adresses sont principalement exprimées sous forme hexadécimale.

Le mécanisme CSMA/CD

Étant donné que toutes les stations d’un réseau local sont sur le même support, il est nécessaire de contrôler l’utilisation de ce dernier. Ethernet emploie donc une méthode d’accès partagé par écoute de la porteuse et détection de collision, appelée CSMA/CD (*Carrier Sense Multiple Acces with Collision Detection*). Son principe est simple: attendre que le support soit libre pour transmettre et détecter les collisions.

Unicast, multicast et broadcast

Une station dispose de trois méthodes pour envoyer des trames:

- **L'adressage broadcast.** La trame est envoyée à toutes les stations du domaine de broadcast.
- **L'adressage multicast.** La trame est envoyée à un sous-ensemble de stations du domaine de broadcast qui appartiennent à un groupe prédéfini.
- **L'adressage unicast.** La trame est envoyée à une seule station spécifique.

Support de transmission partagé

Ethernet suit plusieurs modèles de câblage, dont 10Base2, 10Base5, 10BaseT, 100BaseTX ect... Les stations sont raccordées physiquement à un équipement d'interconnexion (switch, routeur,...) pour former une topologie physique en étoile. Limité, au début, à une vitesse de 10 Mbit/s, la bande passante d'Ethernet passe à 100 Mbit/s, en 1995, avec la publication du standard 802.3u, puis à 1000 Mbit/s, en 1999, avec le standard 802.3z. Je n'entrerai pas dans les détails, mais il est important de signaler que ces standards jouissent une compatibilité descendante (une station au standard 802.3u peut communiquer avec une station 802.3z).

LES LAN SANS FIL 802.11 (WLAN)

Le marché des produits dotés d'une technologie WLAN est en plein essor. Aujourd'hui, les ordinateurs portables, un nombre croissant de téléphones mobiles et les consoles de jeux sont dotés de cette technologie. Tous les fournisseurs d'accès à Internet proposent des solutions domestiques sans fil. La principale raison de cette forte croissance est la facilité d'implémentation d'un réseau sans fil, et la baisse des coûts de cette technologie.
Je vais maintenant explorer la technologie qui se cache derrière le très populaire "Wi-Fi™", nous verrons que son architecture est loin d'être évidente.

Les défis des WLAN

Nous avons vu, dans le chapitre précédent, que les réseaux Ethernet sont pourvus d'une technologie (CSMA/CD) pouvant détecter les collisions. Les stations 802.11 n'en sont pas pourvues. Il faut donc mettre en place une autre technique afin d'éviter que deux stations "se parlent" en même temps. La sous-couche MAC, doit elle aussi fournir un accès équitable au support sans fil et doit donc offrir davantage de fonctions tout en restant évolutive.

La sécurité est le problème crucial des réseaux sans fil : n'importe quel appareil équipé, se trouvant dans la zone de couverture d'un réseau sans fil, peut capter les trames transmises sur le support radio. Des systèmes d'authentification et de chiffrement, que nous évoquerons plus loin, sont indispensables.

Les topologies de réseaux sans fil

Les WLAN de norme 802.11 offrent trois types de topologies pour concevoir un WLAN:

- **L'IBSS** (Independent Service Set)
- **Le BSS** (Basic Service Set)
- **L'ESS** (Extended Service Set)

Un ensemble de service (Service Set) consiste en un groupement logique d'équipements.

Dans un réseau sans fil, les données sont transmises sur une porteuse radio. Il est fréquent d'une station réceptrice d'une groupe se trouve dans la même plage de fréquence de plusieurs stations émettrices d'autres groupes. Afin de trier les signaux reçus, la station émettrice préfixe un identifiant de service set, appelé SSID (*Service Set Identifier*), aux données à transmettre.

Un **IBSS** est un ensemble de stations communiquant directement entre elles. Un WLAN **IBSS** (aussi appelé *ad hoc*) est donc formé par au moins deux stations, et représente un réseau autonome. Les clients sont directement reliés les uns aux autres. La synchronisation est gérée par les clients eux-mêmes, je ne détaillerai pas ce processus ici. Ce genre de réseau est généralement petit et n'est utilisé, en général, que pour l'échange occasionnel de fichiers.

Un **BSS** est un ensemble de stations communiquant entre elles via l'intermédiaire d'une station spéciale, appelée AP (*Acces Point* ou *point d'accès*). L'AP peut disposer d'une connexion (*uplink*) vers un réseau câblé, on est alors dans le cas d'un BSS d'infrastructure. Cette topologie est généralement utilisée pour un réseau domestique.

Un **ESS** est un ensemble de BSS interconnecté via un système de distribution (DS pour *Distribution System*). La plupart du temps, le DS est un réseau câblé. Cette topologie est notamment utilisée à l'Université de Genève.

L'accès au support

Pour détecter les collisions, les WLAN 802.11 utilisent une méthode proche de celle des réseaux Ethernet 802.3: l'accès partagé par l'écoute de la porteuse, ou **CMSA/CA** (*CMSA with Collision Avoidance*). Cela consiste, pour une station, à écouter le support pour détecter s'il y a un signal porteur et attendre, si c'est le cas, qu'il soit libre avant de transmettre. Sur un réseau Ethernet, lorsque deux stations émettent simultanément, le niveau du signal sur le câble augmente, leur indiquant qu'une collision à lieu. Les WLAN n'ayant évidemment pas cette capacité, le mécanisme d'accès est pensé pour éviter les collisions.

Si nous comparions le principe **CMSA/CA** à une audioconférence, voici comment, selon le livre “Réseaux WiFi: notions fondamentales”, (cf. Bibliographie), elle se déroulerait cette dernière:

“

- *Avant de prendre la parole, un participant indique pendant combien de temps il compte occuper le canal, donnant une idée aux autres participants de leur durée d’attente avant de pouvoir s’exprimer à leur tour.*
- *Aucun participant ne peut intervenir avant que le temps de parole du participant en cours soit écoulé.*
- *Un participant ne peut savoir que sa voix a été entendue par les autres participants que s’il en reçoit la confirmation.*
- *Si deux participants parlent en même temps, ils l’ignorent. Le fait de ne par recevoir de confirmation leur indique toutefois qu’ils n’ont pas été entendus.*
- *Lorsqu’un participant ne reçoit pas de confirmation, il patiente pendant une durée aléatoire puis tente de parler de nouveau.*”

Une collision est donc détectée implicitement lorsque l’émetteur ne reçoit pas l'acquittement de son envoi. Je ne détaillerai pas l’implémentation relativement complexe de CMSA/CA car elle prendrait deux fois la taille de ce projet.

Une autre caractéristique importante des réseaux sans fil est la fragmentation des trames qui est une fonction de la sous-couche MAC, elle vise à augmenter la fiabilité des transmissions en décomposant chaque trame en fragment plus petit envoyé individuellement. Le principe étant qu’un petit fragment a plus de chances d’être transmis correctement. De plus, si un fragment subit une altération ou une collision, seul le fragment, et non la trame entière, doit être retransmis.

Les fonctions de la sous-couche MAC 802.11

Nous savons maintenant comment les stations 802.11 se partagent l’accès au réseau sans fil. Voyons a présent comment les stations 802.11 choisissent un

AP et communiquent avec lui et comment fonctionne le mode d'économie d'énergie.

Voici les trois échanges requis entre une station est un AP pour communiquer:

- Le processus de **sondage**, ou probe;
- Le processus d'**authentification**;
- Le processus d'**association**.

Le processus de sondage, consiste généralement, à émettre une trame de requête probe sur chaque canal (1 à 13 en Europe). Cette trame contient notamment des informations sur la station émettrice (les plus importantes sont les débits supportés (**IE Supported Rates** et l'ensemble de services auquel elle appartient (**IE SSID**)). Ce processus à pour but de permettre à la station de connaître les AP qui se trouvent à proximité.

Lorsqu'un AP reçoit une telle requête, il répond par une trame de réponse probe dont les champs principaux sont:

- **Le Timestamp**: c'est la valeur du temporisateur TSF qui sert à synchroniser l'horloge de la station avec celle de l'AP
- **Le Beacon Interval**: contient le nombre d'unités de temps entre les trames de balisage.
- **Le Capability Information**: contient les informations sur les capacités des couches MAC et PHY.
- **L'IE SSID**: contient le SSID avec lequel l'AP est configuré.
- **L'IE Supported Rates**: indique les débits supportés par l'AP.
- **L'IE PHY Parameters**: fourni à la station des informations spécifiques à la couche PHY.

Lorsque la station reçoit les trames de réponse probe des AP, elle peut, suivant la configuration, se connecter automatiquement à un AP ou alors attendre la décision de l'utilisateur de la station.

Le processus d'authentification est très important dans les WLAN, il permet de déterminer qui est autorisé à accéder au réseau. Le standard 802.11 possède deux modes différents: Open System et Shared Key que j'aborderai plus tard. Pour simplifier, la station envoie une requête d'authentification et l'AP lui renvoie une réponse d'authentification.

Le processus d'association autorise ou non un AP à assigner un port logique à la station sans fil. Il est initié par la station au moyen d'une trame de requête et se termine par une réponse de l'AP lui indiquant le succès ou l'échec.

Une des fonctions intéressantes de la sous-couche MAC 802.11, mais que je ne détaillerai pas, est l'économie d'énergie. Le principe est simple; la station désactive son dispositif sans fil. L'AP auquel elle est associée met alors les trames destinées à la station dans un tampon. À intervalles réguliers, la station réactive le dispositif radio et attend l'arrivée d'une trame beacon d'AP lui indiquant la présence de trames à son intention. En mode unicast, un intervalle d'écoute ou de réveil est défini par le client.

La couche physique 802.11

La couche physique (couche 1 du modèle OSI) est chargée de gérer les connexions matérielles. Elle est divisée en deux parties: **PLCP** (*Physical Layer Convergence Protocol*) et **PMD** (*Physical Medium Dependant*).

L'encapsulation[4] des informations fournies par la couche liaison de données est réalisée par la sous-couche PMD grâce à deux méthodes: il faut, en premier lieu, choisir une méthode de transmission des informations, puis une méthode de codage.

Pour que les stations puissent communiquer entre elles, le standard 802.11 définit trois couches physiques:

- **Le FHSS** (*Frenquency Hopping Spread Spectrum*)
- **Le DSSS** (*Direct Sequence Spread Spectrum*)
- **L'IR** (*Infra-Red*) que nous ne détaillerons pas.

4 cf. glossaire

La technique DSSS consiste à émettre sur plusieurs fréquences données, on appelle cela “étalement du spectre”. La bande allant de 2’400 à à 2’483,5 MHz est divisée en quatorze canaux de 20 MHz chacun. L’émetteur et le récepteur communiquent sur un canal sélectionné (donc sur plusieurs fréquences). C’est sur cette technique que s’appuie la norme 802.11. Elle a pour avantage d’augmenter le débit en utilisant, au mieux, la bande passante, mais est très sensible aux interférences. La grande popularité des appareils Wi-Fi™ a eu pour effet, selon la presse spécialisée, de générer des saturations dans les WLAN de plusieurs zones urbaines, leurs utilisateurs souffrent alors d’un débit amoindri.

La technique FHSS, quant à elle, consiste à découper la bande de fréquence en septante-neuf canaux afin de “sauter” d’une fréquence à une autre. Ce découpage nécessite de l’AP et de la station une synchronisation sur une séquence de sauts précise. Ces derniers s’effectuent, en général, toutes les 300 à 400 ms. L’objectif étant la diminution de collisions de trames lorsque plusieurs stations sans fil sont dans la même zone géographique. Beaucoup moins sensible aux interférences, cette technique est notamment utilisée par la technologie Bluetooth™[5].

Les WLAN 802.11b utilisent le DSSS haut débit (HR-DSSS) en utilisant des techniques de modulations supplémentaires pour arriver à un débit de 11Mbit/s.

Les WLAN 802.11g introduisent la couche ERP (*Extended Rate Physical*) pour atteindre des débits atteignant 54Mbit/s. Diverses autres techniques de modulation sont utilisées pour arriver à un tel débit.

Les trames 802.11

Nous abordons ici brièvement l’aspect des trames 802.11 DSSS.
Elles contiennent quatre champs principaux:

- **Le préambule.** Il contient deux éléments différents: *Synch.* qui est une séquence de 128 bits utilisée pour la détection et la synchronisation et *SFD* (*Start Frame Delimiter*) qui détermine le début de la trame.

5 cf. glossaire

- **L'en-tête PCPL.** Contient quatre sous-champs. Le premier, appelé *Signal*, indique la modulation qui doit être utilisé pour la transmission et la réception des données MAC. Le second, nommé *Service*, n'est pas encore utilisé par le standard 802.11. Le troisième champ, intitulé *Lenght*, indique le nombre d'octets que contient la trame. Enfin, le dernier champ appelé *CRC* (*Cyclic Redundancy Check*), permet la détection d'erreurs de transmission.

- **Les données MAC.** Cette partie sera détaillée ci-dessous.

- **Le CRC.** Contient un code binaire généré pour l'envoi afin de détecter la présence d'erreurs survenues lors de la transmission.

A noter que dans la cas du DSSS, le préambule peut être court ou long et que les trames PLCP sur FHSS sont légèrement différentes.

Les trames 802.11 au niveau de la couche MAC sont divisées en trois grandes parties:

- **L'en-tête.** Il contient le *Contrôle de trame* (que nous détaillerons plus loin), la *Durée/ID* qui indique la valeur d'une durée ou l'ID de la station dans le cas d'une trame de pooling, *Adresse 1* qui est l'adresse du récepteur, *Adresse 2* qui est l'adresse de l'émetteur, *Adresse 3* qui est l'adresse de l'émetteur original ou celle de destination, le *Contrôle de séquence* qui est utilisé pour représenter l'ordre des différents fragments appartenant à la même trame et reconnaître des objets dupliqués, et, enfin, *Adresse 4* qui est utilisée lors d'une transmission d'un AP à un autre.

- **Le corps de la trame.** Contient des informations sur couche supérieure.

- **CRC.** Calculé à partir de l'en-tête MAC afin de détecter d'éventuelles erreurs de transmission.

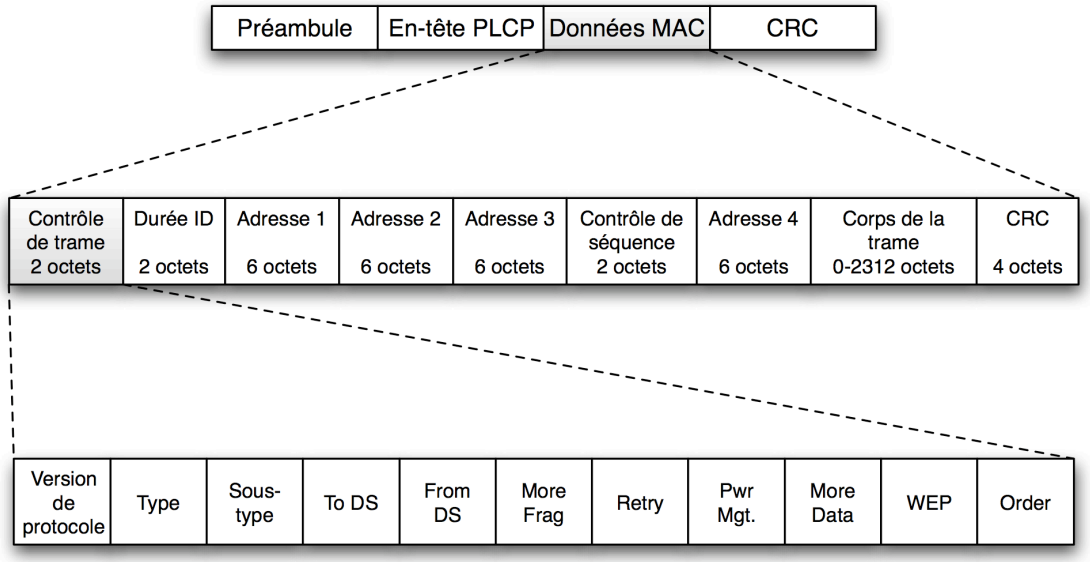
Le *Contrôle de trame* est utilisé pour définir le type d'information envoyé. Voyons à présent de quoi est constitué.

- **Version de protocole.** Ce champ contient 2 bit qui pourront être utilisés pour reconnaître des versions futures possibles du standard 802.11. Dans la version actuelle, la valeur est fixée à 0.

- **Type et sous-type.** Ils définissent le type et sous-type des trames.

- **ToDS.** Bit, dont la valeur est 1 lorsque la trame est adressée à l'AP pour qu'il la fasse suivre au DS (*Distribution System*).
- **FromDS.** Bit dont la valeur est 1 lorsque la trame provient du DS.
- **More Fragments.** Bit, dont la valeur vaut 1 lorsque d'autres fragments suivent le fragment en cours.
- **Retry.** Ce bit indique si le fragment est une retransmission.
- **Power Management.** Ce bit indique si la station sera en mode d'économie d'énergie après la transmission de cette trame.
- **More Data.** Également utilisé pour la gestion de l'énergie, ce champ est employé par l'AP pour indiquer que d'autres trames sont stockées dans la mémoire tampon pour cette station.
- **WEP.** Ce bit indique si le corps de la trame est sécurisé ou non.
- **Order.** Ce bit indique si cette trame est envoyée en utilisant la classe de service strictement ordonnée. Cette classe est définie pour les utilisateurs qui ne peuvent accepter de changement d'ordre entre les trames unicast et multicast.

Voici la représentation graphique d'une trame 802.11 DSSS:



Trame 802.11 DSSS

La sécurité des WLAN

La sécurité est le plus gros problème des réseaux sans fil. Les équipements 802.11 communicants par onde radio, ils couvrent une zone plus étendue qu'on ne le désirerait. Les AP transmettent les données en broadcast dans l'espoir que la station réceptrice opère dans la même plage de fréquences, n'importe quelle autre station opérant dans cette même plage reçoit aussi ces données. Bon nombre de personnes ayant acquis un équipement 802.11, ne sachant pas sécuriser leurs réseaux, laissent une porte grande ouverte à leurs voisins. Il est, en effet, on ne peut plus simple de se connecter à un réseau dit "ouvert" pour utiliser la connexion internet ou encore explorer le contenu des ordinateurs attachés à ce réseau.

Deux composants sont requis pour assurer une sécurité minimale à un WLAN:

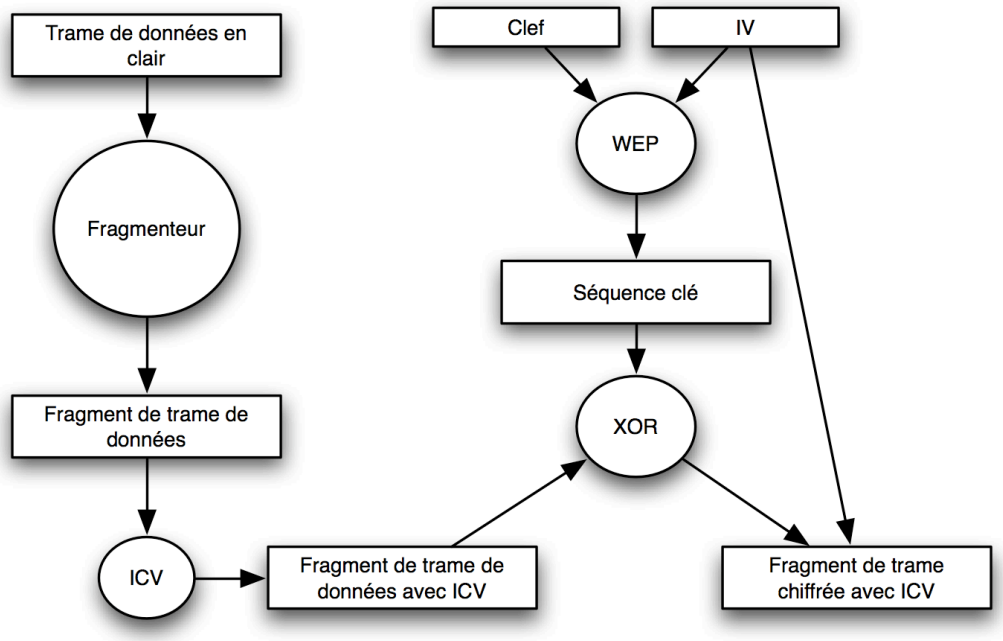
- Un moyen de déterminer qui peut exploiter le WLAN.
- Un moyen de garantir la confidentialité des données transmises.

La première exigence est assurée par des mécanismes d'authentification permettant le contrôle d'accès au réseau local. La seconde est satisfaite par des algorithmes de chiffrement. Les spécifications 802.11 définissent plusieurs algorithmes de chiffrement, dont WEP (*Wired Equivalent Privacy*) et WPA (*Wi-Fi Protected Acces*) qui sont les plus populaires, ainsi que deux méthodes d'authentification: Open System Authentification et Shared Key Authentification.

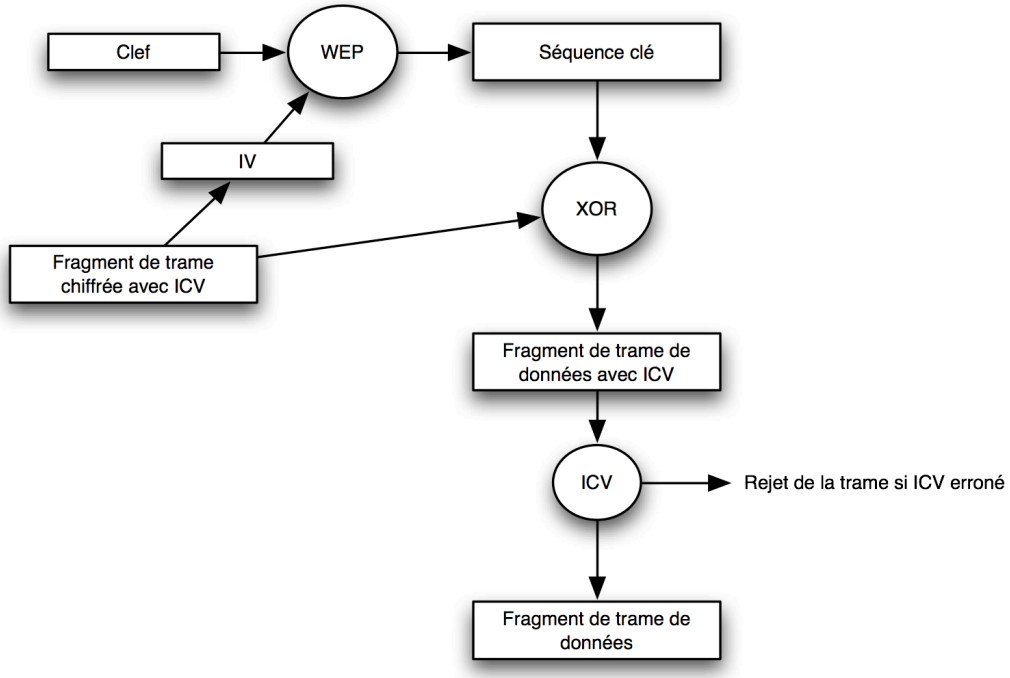
Les algorithmes WEP et WPA utilisent un algorithme de chiffrement par flot RC4. Également utilisé dans SSL, cet algorithme fonctionne de la façon suivante[6]: "*la clef RC4 permet d'initialiser un tableau de 256 octets en répétant la clef autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées : les octets sont déplacés dans le tableau, des additions sont effectuées, ect. Le but est de mélanger autant que possible le tableau. Au final, on obtient une suite de bits qui parait tout à fait aléatoire. Par la suite, on peut extraire des bits par conséquent pseudo-aléatoires.*"

6 http://fr.wikipedia.org/wiki/RC4

Je ne détaillerai pas le processus de chiffrement et de déchiffrement WEP et WPA, mais voici quand même un tableau récapitulatif représentant le processus dans le cas du WEP (IV est le vecteur d'initialisation et ICV sert à contrôler l'intégrité de la trame):



Processus de chiffrement WEP



Processus de déchiffrement WEP

Abordons maintenant les deux mécanismes d'authentification spécifiés par le standard 802.11. L'authentification Open System repose sur un algorithme qui accepte toutes les requêtes d'authentification. Le contrôle d'accès, avec l'authentification Open System, s'appuie sur la clé WEP ou WPA utilisée par l'AP et le client. Ils ne peuvent communiquer que s'ils ont la même clef, dans le cas contraire, les trames sont supprimées par le client et par l'AP. Si ce dernier n'a pas été configuré pour utiliser une clef de chiffrement, n'importe quel équipement peut accéder au WLAN et les trames sont transmises sans être cryptées.

L'authentification Shared Key exige que le chiffrement soit activé avec une même clef sur le client et l'AP. Voici les étapes du processus tiré du livre "Réseaux WiFi: notions fondamentales" (cf. Bibliographie):"

1. *Le client envoie à l'AP une requête pour l'authentification Shared Key.*
2. *L'AP répond avec un texte-challenge en clair.*
3. *Le client chiffre le texte-challenge et place le résultat dans une trame de réponse.*
4. *Si l'AP peut déchiffrer la trame et extraire le texte-challenge initial, le client reçoit un message de réussite.*
5. *Le client peut accéder au WLAN."*

Contrairement à l'authentification Open System, le mode Shared Key requiert que le chiffrement soit activé sur l'AP et la station pour permettre au client de s'associer.

En complément à ces deux modes d'authentification spécifiés par le standard 802.11, de plus en plus de fabricants proposent l'authentification par adresse MAC. Le principe est simple; il consiste à configurer l'AP avec une liste des adresses MAC des stations autorisées à accéder au réseau. Lors de l'authentification, l'AP compare l'adresse MAC du client effectuant la requête avec celles étant dans sa liste des adresses autorisées, le processus d'authentification continue uniquement si l'adresse du client est présente dans cette liste.

Les failles du standard 802.11

Nous venons de survoler les différentes stratégies de sécurités des WLAN. Elles n'en restent, cependant, pas inviolables. En voici, d'ailleurs, les différentes vulnérabilités de ces mécanismes.

L'authentification Open System, comme cela a déjà été dit, ne permet pas de vérifier si un client voulant se connecter à l'AP est autorisé à le faire. N'importe qui peut donc accéder au réseau.

Plus ennuyeux, l'authentification Shared Key présente une faille importante. Comme cela a été exposé préalablement, il y a, durant l'authentification, transmission en clair d'un texte challenge par l'AP, celui-ci est ensuite renvoyé chiffré par le client. N'importe quelle station, se trouvant dans la zone de couverture peut recevoir ces deux textes. Il a aussi été dit que la séquence clef et le texte sont combinés au moyen d'un "ou exclusif" (l'opérateur booléen XOR) dans le processus de chiffrement WEP. Si l'attaquant capture le texte challenge et le texte chiffré, il lui suffit d'appliquer l'opération XOR pour découvrir la séquence clé. Il peut alors déchiffrer les trames de même longueur que la séquence, à condition que le vecteur d'initialisation (IV) utilisé pour produire cette dernière soit le même que celui ayant servi à chiffrer la trame.

L'authentification par adresse MAC n'est pas infaillible non plus. Les adresses MAC sont transmises en clair dans les trames 802.11. Lorsqu'un client a accès au réseau, il est alors possible de connaître son adresse MAC en collectant une trame. Certaines cartes réseau 802.11, permettent de remplacer l'adresse MAC imposée par le fabricant (*UAA - Universally Administered Address*) par une adresse voulue (*LAA - Locally Administered Address*). Il s'agit donc d'usurpation de l'adresse MAC d'un client valide.

Le problème de sécurité le plus important concerne le chiffrement WEP. Il est en effet possible, en collectant passivement quelques centaines de milliers de trames d'un WLAN, de connaître la clef WEP de ce dernier. Sur un WLAN à fort trafic, cette opération peut être faite en quelques heures. Cette faille a trait à la façon dont WEP implémente un des algorithmes de RC4. Un certain nombre de vecteurs d'initialisation (IV) permettent d'obtenir des octets de la clef WEP par analyse statistique. Il existe, aujourd'hui, des programmes collectant

automatiquement le nombre de trames nécessaire et délivrant instantanément la clef WEP.

Pour pallier à ces problèmes, l'IEEE a développé des extensions améliorant la sécurité au sein des WLAN. Inclus dans la norme 802.11i ratifiée en 2003, le WPA est une solution pour corriger les problèmes du WEP. Il est maintenant supporté par tous les fabricants d'équipement WLAN.

Sans entrer des les détails, l'implémentation WPA a été prévue pour être utilisée avec un serveur d'identification 802.1X distribuant différentes clefs à chaque utilisateur. Il peut aussi être utilisé en mode PSK (*Pre-Shared Key*), mode dans lequel une clef partagée est utilisée. Il utilise, comme WEP, un chiffrement par flot RC4 avec une clef de 128 bits et un vecteur d'initialisation (IV) de 48 bits. Le principal atout du WPA est le protocole TKIP (*Temporal Key Integrity Protocol*) qui a pour but d'échanger dynamiquement les clefs lors d'une utilisation du système. De plus, WPA possède un algorithme d'intégrité des données amélioré qui permet à un récepteur de détecter les altérations potentielles du contenu d'une trame depuis son émission. Le WPA comporte malgré tout des faiblesses: il est possible de contourner le protocole TKIP, mais cela nécessite une importante quantité de calcul (de l'ordre de 30'000 jours sur un Pentium 4)[7].

Dernière évolution en matière de chiffrement: le WPA2. Il utilise un chiffrement plus poussé basé sur AES plutôt que sur RC4.

Sujets annexes non développés

Il existe d'autres sujets concernant les WLAN que je vais citer à présent.

La mobilité figure parmi les concepts fondamentaux des WLAN. Elle désigne la capacité des hôtes à se déplacer. Le terme *roaming* est utilisé pour qualifier les déplacements. Il existe deux types de roaming: le roaming tranparant et le roaming nomade. Le premier est celui que l'on rencontre dans les réseaux de téléphonie cellulaire (GSM). Le second s'applique à des équipements dans un

7 Source: http://fr.wikipedia.org/wiki/WPA

environnement 802.11: l'utilisateur n'exploite le service réseau que lorsqu'il atteint sa destination, et non pendant son déplacement.

Autre caractéristique importante des WLAN: la qualité de service (*QoS*). Indispensable pour la transmission de flux audio ou vidéo, il s'agit donner la priorité à ce type de données qui sont sensibles aux retards de transmission.

Autres sujets non évoqués, mais qu'il est tout de même important de nommer ici: les notions essentielles sur la transmission radio afin de comprendre et d'évaluer les informations de niveau physique et le déploiement des WLAN, la variation automatique de débit, les autres normes 802.11 moins répandues ainsi que l'impact sur la santé des ondes radio.

Le futur des WLAN: 802.11n et WiMAX

Promis pour 2007[8], le standard 802.11n implémente la technologie MIMO (*Multiple Input Multiple Outpout*) afin de promettre un débit de l'ordre des 600 Mbits/s et une portée améliorée par rapport au standard 802.11g. Des fabricants proposent, depuis plusieurs mois déjà, des produits "Draft-N". Ce standard devrait vite remplacer le 802.11g dans les réseaux domestiques.

WiMAX[9] (*Worldwide Interoperability for Microwave Acces*) est une famille de normes, dont certaines sont encore en discussion. Elle regroupe des standards de réseaux sans fil et promet des débits de plusieurs dizaines de mégabits par seconde sur des rayons de couvertures de plusieurs dizaines kilomètres. WiMAX utilise des technologies hertziennes destinées principalement à des architectures point-multipoint : à partir d'une antenne centrale, on cherche à toucher de multiples terminaux. Le paragraphe suivant, emprunté à Wikipedia, donne les utilisations prévues de WiMAX:

"*WiMAX est envisagé à la fois pour les réseaux de transport et de collecte, et pour les réseaux de desserte. Dans le cas de la collecte, il s'agit du backhauling de hotspots, c'est-à-dire la liaison des hotspots Wi-Fi à Internet non pas par des dorsales filaires (ADSL notamment), mais par une dorsale hert-*

8 Source: http://www.canardwifi.com/index.php?2006/08/16/1566-retards-pour-la-norme-80211n

9 Source: http://fr.wikipedia.org/wiki/Wimax

zienne. Dans le cas de la desserte, c'est l'idée, et notamment pour les aspects mobilité de WiMAX, que des hotspots (des hotzones, en fait) soient déployées sous technologie WiMAX."

CONCLUSION

La technologie des réseau Wi-Fi™ est une véritable révolution dans le monde de l'informatique. Pouvoir être connecté à un réseau, connu ou non, sans avoir à se soucier du câblage est, en effet, un atout indéniable.

Depuis l'an 2000, l'Université de Genève déploie une structure WLAN dans ses bâtiments, celle-ci est d'ailleurs utilisée par un nombre considérable d'étudiants et de professeurs. Cette solution est plus aisée et moins onéreuse à mettre en place que l'installation de prise dans chaque espace de travail.
L'essort de cette technologie dépasse nos frontières, une communauté à l'échelle mondiale (FON[10]) à même été fondée afin de permettre le partage des connexions internet domestiques, cela via un réseau Wi-Fi™.
Certains produits, comme les "Media Center"[11], ont d'ailleurs vu leurs ventes augmenter[12] avec la ratification du standard 802.11g.
Il faut également noter que les équipements Wi-Fi™ à usage domestique doivent leurs démocratisation en grande partie à leur simplicité d'utilisation.

Si le Wi-Fi™ a encore de beaux jours devant lui, il ne présente, pour autant, pas que des avantages. Son utilisation présente de gros risque au niveau de la sécurité rendant ce type de communication peu sûr. Lorsqu'il s'agit de transférer ou conserver des données sensibles sans cryptage particulier (numéros de carte de crédit, e-banking, emails confidentiels), il vaut mieux préférer le bon vieux câble réseau.

Fait non évoqué dans ce projet, la différence entre le débit théorique et le débit effectif, qui peut être importante, dépend de nombreux paramètres. Il est, par exemple, difficile de faire du streaming vidéo haute définition en utilisant un réseau 802.11g, alors que son débit théorique le permet parfaitement. La paire torsadée a donc, elle aussi, un avenir certain et cela principalement dans le milieu professionnel.

---

10 http://fr.fon.com

11 cf. glossaire

12 Exemple avec l'Apple TV: http://www.macbidouille.com/news/2007-01-26/#13905

BIBLIOGRAPHIE

Livres:

Pejman Roshan, Jonathan Leary. Réseaux WiFi: notions fondamentales. Cisco Press, 2004

Thibaud Schwartz. Réseaux Wi-Fi. Micro Application, 2003.

Paul Mühlethaler. 802.11 et les réseaux sans fil. Eyrolles,2002.

Matthew S. Gast. 802.11 : réseaux sans fil : la référence. O'Reilly, 2005

Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. Wi-Foo : piratage et défense des réseaux sans fil. CampusPress, 2005.

Sites Internet:

www.wi-fi.org

www.hsc.fr

www.wikipedia.org

www.commentcamarche.net

www.clubic.com

www.linternaute.com/hightech/wifi/

www.zdnet.fr/special/wi-fi/

GLOSSAIRE

Bluetooth™: Emprunté à Wikipedia: "*Bluetooth est une spécification de l'industrie des télécabineommunications. Elle utilise une technologie radio courte distance destinée à simplifier les connexions entre les appareils électroniques. Elle a été conçue dans le but de remplacer les câbles entre les ordinateurs et les imprimantes, les scanners, les claviers, les souris, les téléphones portables, les PDAs et les appareils photos numériques.*"

Encapsulation: Procédé consistant à inclure les données de la couche d'un protocole donné afin que la couche d'un protocole de plus bas niveau en face abstraction. Par exemple[13], un fragment de donnée est encapsulé dans un datagramme UDP (*User Datagram Protocol*) qui lui même est encapsulé dans un paquet IP, ce dernier étant alors envoyé via un protocole de la couche de liaison , comme par exemple Ethernet.

IEEE: Institute of Electrical and Electronics Engineers. C'est une organisation qui a pour but de promouvoir la connaissance dans le domaine de l'ingénierie électrique.

LAN: Local Area Network

Media Center: Système, généralement équipé Wi-Fi™, dont la fonction est la lecture de fichier multimédia.

Streaming: Lecture en continu.

Trame: paquet d'information véhiculé au travers d'un support physique.

Wi-Fi™: Wireless Fidelity

WLAN: Wirless Local Aera Network

13 Emprunté à Wikipedia