TD - Les réseaux WIFI

1. Introduction aux réseaux sans fil

1.1 Définition d'un réseau sans fil

Un **réseau sans fil** (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux (ordinateur portable, PDA, etc.) peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

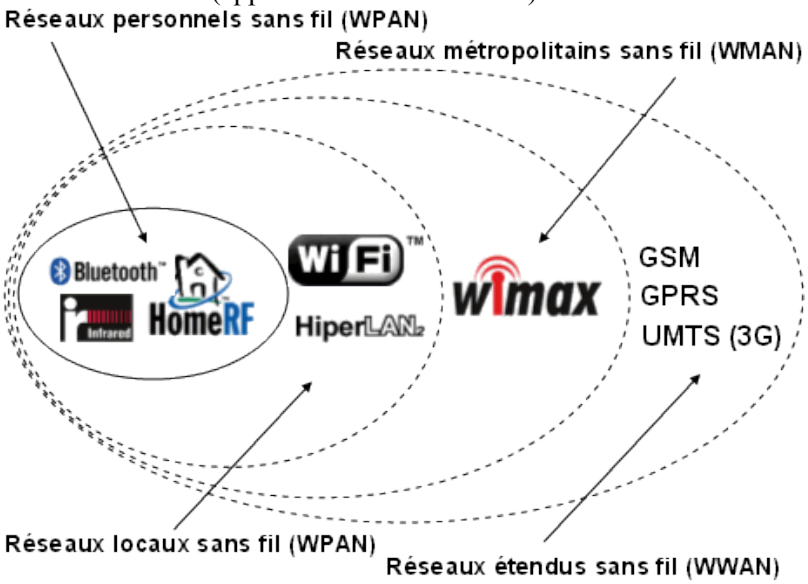
Les réseaux sans fil sont basés sur une liaison utilisant des **ondes radioélectriques** (radio et infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions.

Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires (creusement de tranchées pour acheminer les câbles, équipements des bâtiments en câblage, goulottes et connecteurs), ce qui a valu un développement rapide de ce type de technologies.

En contrepartie se pose le problème de la réglementation relative aux transmissions radioélectriques. En effet, les transmissions radioélectriques servent pour un grand nombre d'applications (militaires, scientifiques, amateurs, ...). Elles sont sensibles aux interférences, c'est la raison pour laquelle une réglementation est nécessaire dans chaque pays afin de définir les plages de fréquence et les puissances auxquelles il est possible d'émettre pour chaque catégorie d'utilisation.

De plus les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc facile pour un pirate d'écouter le réseau si les informations circulent en clair. Il est donc nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil.

On distingue habituellement plusieurs catégories de réseaux sans fil, selon le périmètre géographique offrant une connectivité (appelé zone de couverture) :



2. Présentation de WIFI

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom Wi-Fi (contraction de Wireless Fidelity,

parfois notée à tort WiFi) correspond initialement au nom donnée à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wifi est en réalité un réseau répondant à la norme 802.11. Les matériels certifiés par la Wi-Fi Alliance bénéficient de la possibilité d'utiliser le logo suivant :

Couche Liaison de données (MAC)	802.2						
	802.11						
Couche Physique(PHY)	802.11 DSSS	802.11 FHSS	802.11 IR	802.11a	802.11b	802.11g	…

2.1 Les différentes normes WIFI

Nom de la norme	Nom	Description
802.11a	Wi-Fi 5	La norme 802.11a (baptisée Wi-Fi 5) permet d'obtenir un haut débit (dans un rayon de 10mètres: 54 Mbit/s théoriques, 30 Mbit/s réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquences des 5 GHz.
802.11b	Wi-Fi	La norme 802.11b est la norme la plus répandue en base installée actuellement. Elle propose un débit théorique de 11 Mbit/s (6 Mbit/s réels) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquences utilisée est la bande des 2,4 GHz avec, en France, 13 canaux radio disponibles.
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquences et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche *liaison de données*. Ainsi, cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de manière à permettre, notamment, une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de points d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming)
802.11g		La norme 802.11g est la plus répandue dans le commerce actuellement. Elle offre un haut débit (54 Mbit/s théoriques, 26 Mbit/s réels) sur la bande de fréquences des 2,4 GHz. La norme 802.11g a une compatibilité descendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b. Cette aptitude permet aux nouveaux équipements de proposer le 802.11g tout en restant compatible avec les réseaux existants qui sont souvent encore en

		802.11b.
802.11h		La norme 802.11h vise à rapprocher la norme 802.11 du standard Européen (Hiperlan 2, d'où le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquences et d'économie d'énergie.
802.11i		La norme 802.11i a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11n	WWiSE (World-Wide Spectrum Efficiency) ou TGn Sync	La norme 802.11n est attendue pour mi Octobre 2009. Le débit théorique atteint les 540 Mbit/s (débit réel de 100 Mbit/s dans un rayon de 90 mètres) grâce aux technologies MIMO (multiple-input multiple-output) et OFDM (Orthogonal Frequency Division Multiplexing). A partir de 2006, des périphériques à la norme 802.11n ont commencé à apparaître mais il s'agit d'un 802.11 N draft (brouillon) ou plutôt provisoire en attendant la norme définitive.
802.11s	Réseau Mesh	La norme 802.11s est actuellement en cours d'élaboration. Le débit théorique atteint aujourd'hui 1 à 2 Mbit/s. Elle vise à implémenter la mobilité sur les réseaux de type adhoc. Tout point qui reçoit le signal est capable de le retransmettre. Elle constitue ainsi une toile au dessus du réseau existant. Un des protocoles utilisé pour mettre en œuvre son routage est OLSR.

2.2 Portées et débits

Les normes 802.11a, 802.11b et 802.11g, appelées «*normes physiques*» correspondent à des révisions du standard 802.11 et proposent des modes de fonctionnement, permettant d'obtenir différents débits en fonction de la portée. Ces valeurs sont données à titre indicatif (dépendent du constructeur, qualité des équipements, puissance du signal, …).

Standard	Bande de fréquence	Débit	Portée
WiFi a (802.11a)	5 GHz	54 Mbit/s	10 m
WiFi B (802.11b)	2.4 GHz	11 Mbit/s	100 m
WiFi G (802.11g)	2.4 GHz	54 Mbit/s	100 m

2.2.1 802.11a

Débit théorique (en intérieur)	Portée
54 Mbits/s	10 m
48 Mbits/s	17 m
36 Mbits/s	25 m
24 Mbits/s	30 m
12 Mbits/s	50 m
6 Mbits/s	70 m

2.2.2 802.11b

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
11 Mbits/s	50 m	200 m
5,5 Mbits/s	75 m	300 m

2 Mbits/s	100 m	400 m
1 Mbit/s	150 m	500 m

2.2.3 802.11g

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
54 Mbits/s	27 m	75 m
48 Mbits/s	29 m	100 m
36 Mbits/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m
6 Mbit/s	90 m	400 m

3. Mise en œuvre de WIFI

3.1 Les équipements

Les principales caractéristiques d'un périphérique WiFi, outre son apparence, sont sa puissance (d'émission) et sa sensibilité (en réception). La puissance en émission détermine en partie la portée du signal émis, ainsi que sa légalité par rapport aux limites autorisées par l'Autorité de Régulation des Télécommunications. La sensibilité est la puissance minimale que doit avoir un signal, à l'arrivée au périphérique, pour que celui-ci puisse le traiter convenablement.

Il existe différents types d'équipement pour la mise en place d'un réseau WIFI :

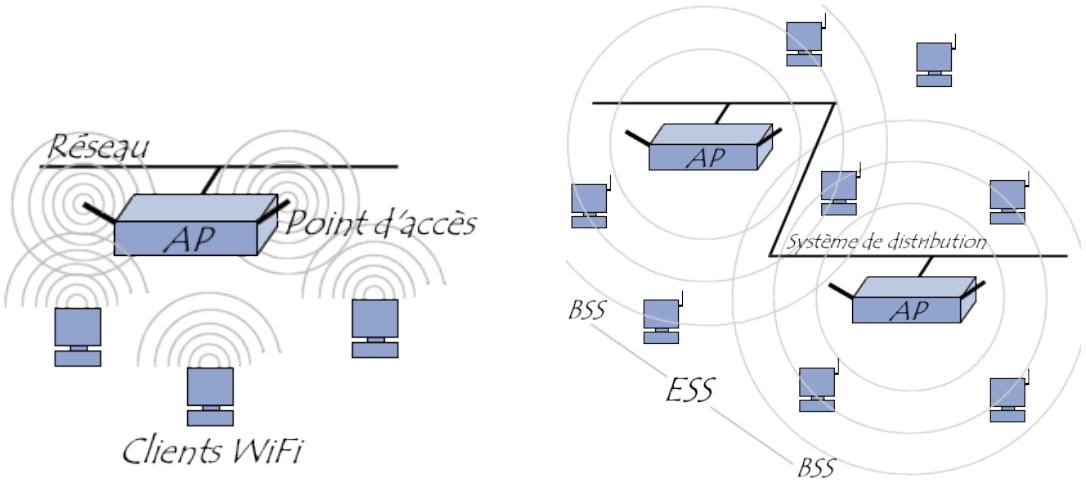
- **Les adaptateurs sans fil ou cartes d'accès WIFI**. Il s'agit d'une carte réseau à la norme 802.11permettant à une machine de se connecter à un réseau sans fil. Les adaptateurs sans fil sont disponible selon différent formats (carte PCI, carte PCMCIA, USB, carte compactflash, technologie Centrino pour les ordinateurs portables, etc.). On appelle **station** tout équipement possédant une telle carte.
- **Les points d'accès ou bornes WIFI**. Un point d'accès permet de donner un accès à un réseau filaire auquel il est raccordé à différentes stations WIFI. Certains équipements proposent des fonctions de modem, de routeur, de firewall, etc.

3.2 Les modes opératoires

3.2.1 Le mode infrastructure

a) Le principe

En mode infrastructure chaque ordinateur station (notée STA) se connecte à un point d'accès via une liaison sans fil.



b) La communication avec le point d'accès

Lors de l'entrée d'une station dans une cellule, celle-ci diffuse sur chaque canal, parmi les 13 canaux radio disponibles, un requête de sondage (probe request) contenant le SSID (Service Set Identifier) pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun SSID n'est configuré, la station écoute le réseau à la recherche d'un SSID.

c) Les Spots

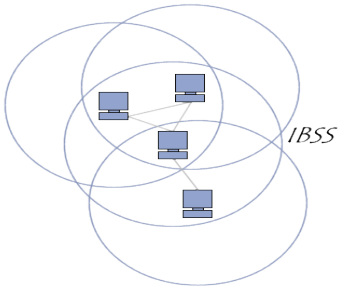
Home Spot : réseau sans fil pour particuliers, qui y trouvent de nombreux avantages tels que l'absence de câble de liaison ou un partage d'accès Internet.

Work Spot : réseau d'entreprise sans fil, en association ou en remplacement d'un LAN Ethernet ; rapidité d'installation et coût inférieur à un réseau filaire.

Hot Spot : réseaux publics en accès libre pour des ordinateurs ou des PDA, géré par des opérateurs téléphonique ou par des entreprises sur des zones publiques (gares, places, restaurants…).

Réseaux associatifs : utilisation, par des associations ou des collectivités locales, de liaison wifi en point à point sur des distances pouvant atteindre quelques kilomètres, dans le but notamment de palier à un manque de ligne ADSL

3.2.2 Le mode ad-hoc



En mode **ad-hoc**, les machines sans fils clientes se connectent les unes aux autres afin de constituer un réseau point à point, c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de station et le rôle de point d'accès.

3.3 Précautions à prendre pour l'installation de WIFI

3.3.1 Attention aux interférences !

Contrairement aux réseaux filaires, les réseaux sans fil requièrent des précautions supplémentaires pour assurer la meilleure propagation possible des ondes. Il est par exemple conseillé de réduire les sources possibles d'interférence comme les appareils Bluetooth ainsi que les fours à micro-ondes. Les obstacles sont aussi des sources d'interférence et d'affaiblissement du signal comme les murs en béton mais aussi le champ électrique d'une télévision.

3.3.2 Attention à la sécurité !

De part la nature des ondes radioélectriques, les réseaux sans fil ne se bornent pas à un périmètre physique limité par des murs. Il est donc nécessaire de mettre en oeuvre un minimum de mécanismes de sécurité.

Une infrastructure adaptée

La première chose à faire lors de la mise en place d'un réseau sans fil consiste à positionner intelligemment les points d'accès selon la zone que l'on souhaite couvrir. Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de réduire la puissance de la borne d'accès afin d'adapter sa portée à la zone à couvrir.

Eviter les valeurs par défaut

Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le mot de passe de l'administrateur. Un grand nombre d'administrateurs en herbe considèrent qu'à partir du moment où le réseau fonctionne il est inutile de modifier la configuration du point d'accès. Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration (généralement via une interface web sur un port spécifique de la borne d'accès) notamment pour définir un mot de passe d'administration.

D'autre part, afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (*SSID*). Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (*broadcast*) de ce dernier sur le réseau. Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé.

Le filtrage des adresses MAC

Chaque *adaptateur réseau* possède une adresse physique qui lui est propre. Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée *ACL*) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines.

Le chiffrement des données

Pour remédier aux problèmes de confidentialité des échanges sur les réseaux sans fils, le standard 802.11 intègre un mécanisme simple de chiffrement des données, il s'agit du **WEP**, Wired Equivalent Privacy. Toutefois, il a été démontré qu'une telle sécurité était facile à contourner.

De nouvelles solutions sont désormais recommandées, comme les méthodes Wi-Fi Protected Access (**WPA**) ou plus récemment **WPA2** depuis l'adoption de la norme **802.11i**.

Il est à noter qu'il existe encore de nombreux Points d'Accès non sécurisés chez les particuliers. Plus de 20 pour cent des réseaux ne sont pas sécurisés.

Références

Introduction aux réseaux WIFI

- Site web http://reseau.erasme.org/rubrique.php3?id_rubrique=38
- Site web www.commentcamarche.net
- Site web http://guide-wifi.blogspot.com/

Réglementation des réseaux WIFI

- Site web http://www.zdnet.fr/produits/materiels/reseau/0,39049804,1005156,00.htm
- Site web http://www.art-telecom.fr/