



## Présentation :

La norme IEEE 802.11 (ISO/CEI 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom wifi correspond initialement au nom donné à la certification délivrée par la 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 (c'est du moins le cas en France, en Espagne, au Canada et aux États-Unis). Ainsi un réseau wifi est en réalité un réseau répondant à la norme 802.11. Dans d'autres pays (en Allemagne par exemple) de tels réseaux sont correctement nommés WLAN.

Grâce au wifi, il est possible de créer des réseaux locaux sans fil à haut débit. Dans la pratique, le wifi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA), des objets communicants ou même des périphériques à une liaison haut débit (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g et 540 Mbit/s pour le futur 802.11n) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres). Dans un environnement ouvert, la portée peut atteindre plusieurs centaines de mètres voire dans des conditions optimales plusieurs dizaines de kilomètres (pour la 'variante' WIMAX ou avec des antennes directionnelles).

Ainsi, des fournisseurs d'accès internet commencent à irriguer des zones à forte concentration d'utilisateurs (gares, aéroports, hôtels, trains, etc.) avec des réseaux sans fil connectés à Internet. Ces zones ou point d'accès sont appelées bornes wifi et en anglais « hot spots ».

Les iBooks d'Apple, Inc. furent, en 1999, parmi les premiers ordinateurs grand public à proposer un équipement wifi intégré (sous le nom d'AirPort), bientôt suivis par le reste de la gamme. À partir de 2003, on voit aussi apparaître des modèles de PC portables bâtis autour de la technologie Intel Centrino, qui leur permettent une intégration similaire. Les autres modèles de PC doivent encore s'équiper d'une carte d'extension adaptée (PCMCIA, USB, Compact Flash, SD, PCI, MiniPCI, etc.).

## Sécurité (confidentialité des communications - risque légal)

L'accès sans fil aux réseaux locaux rend nécessaire l'élaboration d'une politique de sécurité dans les entreprises et chez les particuliers. Il est notamment possible de choisir une méthode de codage de la communication sur l'interface radio. La plus commune est l'utilisation d'une clé dite Wired Equivalent Privacy (WEP), communiquée uniquement aux utilisateurs autorisés du réseau.

Toutefois, il a été démontré qu'une telle sécurité était facile à contourner<sup>3</sup>, avec l'aide de programmes tels que Aircrack.

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.

Ceci peut être combiné avec un accès sécurisé VPN (Virtual Private Network) au réseau dans une entreprise pour limiter le risque d'intrusion.

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[réf. nécessaire]. Il se pose le problème de la responsabilité du détenteur de la connexion wifi lorsque l'intrus réalise des actions illégales sur Internet, comme par exemple télécharger du contenu piraté.

D'autres méthodes de sécurisation existent, avec, par exemple, un serveur Radius chargé de gérer les accès par mot de passe et/ou nom d'utilisateur.

## Travail demandé :

1. Recopiez sur une feuille papier à carreaux, la première partie **PRESENTATION**
2. Donnez les différents débits de transfert en wifi (exemple 11Mbits/s).
3. Expliquez les différentes méthodes pour sécuriser un réseau wifi.