

## Réseaux sans-fil

IFT 3880-IFT 6835 & IFT6802  
Par Laurent Magnin

## Réseaux sans-fil, pourquoi ?

- **Pour offrir une connexion Internet en remplacement du filaire (modem, aDSL)**
  - Satellite
  - Émetteurs terrestres
- **Mobilité chez soi ou en entreprise**
- **Accès depuis des « hot spots »**
  - Gares, cafés, associations bénévoles... avions.
  - Modes gratuits ou avec abonnements
- **Communication directe entre appareils**
  - Échange de cartes d'affaires, etc.

## Technologies de communication

- **Infra-rouge**
  - Faible distance, appareils en vis-à-vis (PDA)
  - Tend à disparaître
- **Téléphone mobile**
- **Bluetooth**
  - Communication hertzienne à courte distance et faible débit
  - Faible consommation électrique

## Technologies de communication (suite)

- **Wi-Fi (*Wireless Fidelity*)**
  - Communication hertzienne à distance moyenne
  - Basée sur le protocole IP (« Internet »)
  - Fourni l'infrastructure des « Hot Spots »
    - Payants (aéroports, etc.)
    - Gratuits mais limités à un lieu (café Wifi)
    - Gratuits (commercial avec publicités ou communautaire)
  - Normes IEEE :
    - IEEE 802.11b : faible débit (< 11Mbps)
    - IEEE 802.11a & 802.11g : débit plus élevé (54Mbps)
    - IEEE 802.11n : débit encore plus élevé (multicanaux)

## Interférences

- **Sur la fréquence 2,4 GHz**
  - Bluetooth
  - IEEE 802.11b et 802.11g (matériels bi-standards)
- **Sur la fréquence 5 GHz**
  - IEEE 802.11a
- **Plus il y a de connexions concurrentes, plus bas est le débit...**
- **802.11g propose une dizaine de canaux**

## Sécurité très faible

- **N'importe qui peut « voir » ce qui transite**
- **N'importe qui peut prendre l'identité d'un autre**
- **À lire : [Myth of Security] !**

### Problèmes posés

- **Accès à Internet sur un réseau autre**
  - Utilisation de la bande passante
  - Actions illégales au nom du propriétaire du réseau
- **Récupération d'informations transmises**
  - Fichiers
  - Mots de passe
- **Intrusion dans le réseau local**
- **(Corruption et modification des données)**

### Augmenter la sécurité ?

- **Restreindre l'accès au réseau**
  - Filtrage de l'adresse « Mac » (*MAC address filtering*)
  - Authentification par mot de passe
- **Encrypter le protocole de communication**
  - Longueur de la clef (minimum 128 bits)
  - Protocole utilisé
    - WEP (très peu sécuritaire)
    - WAP, 802.1X
- **Encrypter les communications**
  - VPN (PPTP, IPSec, OpenVPN)
  - Tunnel (SSH)

### Nouvelles applications (distribuées)

- **Internet, partout, en tout temps !**
  - Accès aux cours de la bourse, à ses courriels...
- **Informatique « située » et personnalisée**
  - En fonction de l'utilisateur et de sa localisation
  - P. ex. : visite touristique, dans un musée, etc.
- **Objets en interaction**
  - Inventaires automatisés dans les magasins (RFID)
  - Appareil photo relié à une imprimante
  - « Matching » dans les bars
  - ...

### Technologies de découverte (de services)

- **Zero Configuration Networking (Zeroconf)**
  - Appelé « RendezVous » par Apple
  - *Allocate addresses without a DHCP server*
  - *Translate between names and IP addresses without a DNS server*
  - *Find services, like printers, without a directory server*
  - *Allocate IP Multicast addresses without a MADCAP server*
- **Jini de Sun**
  - Technologie Java
- **Web Services**
- ...

### Références

- [http://www.oreillynet.com/pub/a/wireless/2003/02/06/wifi\\_products.html](http://www.oreillynet.com/pub/a/wireless/2003/02/06/wifi_products.html)
- <http://www.bluetooth.com/>
- <http://www.arstechnica.com/paedia/w/wireless/security-1.html>
- [Myth of Security]  
<http://www.wirelesspronews.com/wirelesspronews-14-20030827DispellingtheMythofWirelessSecurity.html>
- <http://www.zeroconf.org/>
- <http://www.sun.com/software/jini/>