Réseaux sans fil

Serge Chaumette
Serge.Chaumette@labri.fr

Les différentes technologies

- HomeRF
- Hiperlan
- Bluetooth ou 802.15
- 802.11 ou WLAN

Comparaison Wi-fi / bluetooth

- Wi-fi
- Bluetooth

Principaux problèmes (?)

- Sécurité
- Débit

Pour quelles utilisations ?

- Mobilité
  - Hot spots
  - Réunions, conférences, restaurants, trains, …
- Contraintes physiques
  - Sites classés
  - Entrepôts (grandes surfaces)
- Réutilisation, déménagement du réseau
  - Chantier
  - Expositions temporaires

Pour quels gains ?

- Coût plus faible
  - Matériel
  - Installation
- Installation plus aisée
- Installation plus rapide

Exemples de matériels

VEO Wireless Observer

- http://veo.com/
- http://veo.com/Observer-Wireless/default.asp

[Exemples de matériels]

Wifi Digital Frame

- http://www.wallflower-systems.com/

[Exemples de matériels]

Pèse personne

- IBM et Sunbeam

Nabaztag

- Violet - The Smart Object Company
- http://www.violet.net/

La normalisation

- 1997 : 802.11
- 1999 : 802.11HR
  - Couche physique
    - Débit supérieur
    - Connectivité plus robuste
  - Couche physique
  - Couche liaison de données

Les équipements

- Principaux fournisseurs
- Les points d'accès
- Les stations
- Les antennes

Principaux fournisseurs

- Netgear, Belkin, D-Link, 3Com, Apple, Axis, Bewan, Cisco, HP, Linksys, Olitec, US.Robotics, ZyXEL...
- Cf. le guide Wi-FI de Inmac http://www.inmac.com/

Point d'accès

- Hub ou Switch sans fil
- Si cx sert de pont entre le réseau et le sous-réseau sans fil (WLAN, Wireless Local Area Lan)
  - Notion de SSID
- Alimentation électrique possible via le RJ45 (Power Over Ethernet, POE)

Rappel

- Hub
- Switch

Exemple de point d'accès

- Netgear ME102
- http://www.netgear.com/

Adapteurs Wi-FI

- Clef ou dongle USB
- Cartes PCI
- Cartes ISA
- Cartes PCMCIA
- Cartes CompactFlash
- …
- Autre système embarqué
- …

Exemple de carte PCI

- www.belkin.com
- F5D6001

Exemple de carte PCMCIA

- Netgear MA401

Exemple de carte PCMCIA avec antenne

- Cisco

Adapteur USB 802.11b

- www.olitec.com
- **Adaptateur Wireless 802.11b**
- **Existe aussi en version déportée pour un meilleur positionnement**

Les antennes

- Les antennes de base ne sont pas forcément très efficaces
- Possibilité de se la fabriquer
- Possibilité d'en acheter

Fabriquer son antenne

- Risques
  - Puissance
  - Fréquence

Les différentes normes

802.11b

- 2.4 GHz, 3 canaux
- 11Mbps
- Environ 32 utilisateurs par point d'accès
- Utilisée par les hot spots
- Bande partagée par de nombreuses applications

802.11b+

- Pas une norme
- 22Mbps

802.11a

- Depuis 2002
- 5GHz, 8 canaux sans juxtaposition
- 64 utilisateurs par point d'accès
- 54Mbps
- Portée due à la fréquence plus élevée
- Cohabite avec 11b sans interférence
- Equipements Dual-Band

802.11g

- Normalisation en 2003
- 2.4 GHz avec 3 canaux
- 54Mbps
  - Propriétaires, à upgrader
  - Tous compatibles avec 11b et entre eux en vitesse de 11b

Le standard 802.11

- La couche physique
- La couche liaison de données

La couche physique

- **DSSS** (*Direct Sequence Spread Spectrum, étalement de spectre à séquence directe*)
- FHSS (*Frequency Hopping Spread Spectrum)*
- **PPM** (*Pulse Position Modulation*).

DSSS

- *Direct Sequence Spread Spectrum*
- Utilisation d'une bande spectrale fixe de 22 MHz

DSSS et 802.11

- Plusieurs canaux de 22 Mhz
- Distance entre le début des canaux de 5MHz
- 1 à 11 ou 14 canaux selon la réglementation
- Les canaux se recouvrent ➔ laisser 5 canaux libres entre deux utilisés

FHSS

- *Frequency Hopping Spread Spectrum*
- On découpe la zone spectrale en bandes de largeur égale (hops)
- On émet sur une combinaison connue de toutes les stations de la cellule
  - Pas de sécurité
  - Limitation des interférences

FHSS / DSSS

- FHSS moins gourmand en énergie
- DSSS propose un débit plus important
- DSSS solide/interférence narrow band mais sensible aux interférence large bande

FHSS (suite)

- Dwell time
  - Temps ou on reste sur la même bande
  - Compromis débit/interférences
- Hop time
  - Temps de passage d'une bande à l'autre
  - Compromis coût/temps

FHSS et 802.11

- Normalisation par l'IEEE
  - 1Mb et 2Mb
  - 2,4 – 2,4835 GHz
  - 83 zones de 1MHz
    - 79 disponibles dans la plupart des pays
      - Japon 23
      - Espagne 27
      - France 35 (du 48 au 82)

PPM

- *Pulse Position Modulation*
- Caractère non dissipatif → sécurité
- Impulsions à amplitude constante
- Codage = position de l'impulsion

La couche liaison de données

- *Logical Link Control*, notée **LLC**
- *Media Access Control*, ou **MAC**
  - **CSMA/CA**
    - ***Carrier Sense Multiple Access with Collision Avoidance***
  - **PCF** (Point Coordination Function)

La couche LLC

- LLC 802.2
- Adressage 48 bits

La couche MAC

- En filaire
  - CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
  - Ne marche pas en radio
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance),
  - Réservation du media : Network Allocation Vector
  - Acquittement systématique
    - → coût important
- DCF (Distributed Coordination Function).

- Fragmentation
- Débit variable
- RTS/CTS

Problème du nœud caché

- RTS/CTS
  - Entre la station et le point d'accès
  - Pb. : surcharge le réseau en réservant le support

Ajout de robustesse

- CRC, **Cyclic Redundancy Check**
  - Géré en bas niveau car risques importants
- Fragmentation des paquets
  - Limite le risque de corruption
- Débit variable

La gestion d'énergie

- Traitée par HR
- Deux modes
  - Continuous Aware Mode
  - Power Save Polling Mode

Authentification

- Open system
  - Cas des hotspots
- Shared key
  - Echange d'un message clair puis crypté
  - Cas des réseaux privés

Le roaming

- Deux niveaux
  - Couche 2
    - Protocole propriétaire entre points d'accès
  - Couche 3
    - Mobile IP, IEEE 20002
    - Solution incomplète : DHCP

Les modes de fonctionnement

- Ad'hoc
- Infrastructure ou Access point

Mode Ad'hoc

- Les stations se connectent en point à point
- La communication se fait de toutes vers toutes (graphe complet)
- On parle de IBSS, Independent Basic Service Set

Mode Ad'hoc (suite)

- Il suffit de configurer
  - Le SSID
    - Peut être détecté automatiquement
    - Et donc changé automatiquement ?
  - L'adresse IP
    - Peut être attribuée automatiquement
      - C'est par exemple le cas sous Xp

Mode Ad'hoc (suite)

- Sous Windows
  - ipconfig
- Sous Linux
  - ifcongif
  - iwconfig

Mode Infrastructure

- Il y a un point d'accès connecté au réseau filaire ou pas
- Tous les échanges passent par le point d'accès
- Il peut être la passerelle vers le réseau filaire

Le SSID

- SSID = Service Set Identifier
- Chaque réseau a un nom
  - On peut partager un espace entre plusieurs réseaux
  - Une station peut détecter les réseaux présents
- Il faut séparer les espaces radio des différents réseaux

Les différentes architectures

- BSS, Basic Service Set
  - Un point d'accès
  - Des stations
- ESS, Extended Service Set
  - Partage du même SSID par plusieurs points d'accès sur une même zone
  - Roaming
  - Le client choisit quand changer de point d'accès
  - Hypothèse du même domaine de broadcast

Les différentes architectures (suite)

- IBSS, Independent Basic Service Set
  - C'est le réseau ad'hoc

Sécurité

- Facilité d'accès
- Rogue Access Points
- Utilisation non autorisée des services
- Contraintes de service et de fonctionnement
- MAC spoofing et vol de session
- Traffic Analysis and Eavesdropping
- Attaques de plus haut niveau

Déni de service

- Objectifs
  - Rendre un service inutilisable
- Méthodes
  - Trames de signalisation

Le WEP

- Wired Equivalent Privacy
- Clef privée
- 40 ou 104 bits augmentée d'un vecteur d'initialisation de 24 bits
- VI transporté avec chaque trame
- Ajout d'un contrôle de validité
- Cryptage assuré par rc4

Cryptage par RC4

- Dopage de la clef privée avec le vi
- Création d'une séquence pseudo aléatoire
- Calcul d'intégrité
- Constitution du message final

Sécurité (suite)

- Le war driving (*wardriving* ou *war-Xing*)
- war-chalking

- Cf. Montauban
  - CraieFiti
  - TrebucherSansFil
  - http://www.wifi-montauban.net/

Les outils de la sécurité

- AirSnort
  - http://www.airsnort.com/
- Kismet

AirMagnet

- http://www.airmagnet.com/
- http://www.airmagnet.com/products/handheld.htm

WaveRunner™

- http://www.flukenetworks.com/us/LAN/Handheld+Testers/WaveRunner/Overview.htm

802.11a

- Wifi5
- 54mbps
- 8 canaux
- Bande des 5GHz

802.11b

- Wifi
- 11Mbps
- 3 canaux
- Bande des 2.4GHz

802.11c

- Pontage 802.11 vers 802.11d

802.11d

- internationalisation

802.11e

- Qualité de service au niveau de la couche liaison
- QOS
  - Bande passante
  - Délais

802.11f

- Recommandation pour les vendeurs
- Inter-Access point roaming protocol

802.11g

- 54Mbps
- Bande des 2.4GHz
- Compatibilité avec 802.11b

802.11h

- Cherche à rqprocher le 802.11 su standard européen Hyper Lan 2
- Conformité européenne
  - Fréquence
  - Économie d'énergie

802.11i

- Améliorer la sécurité des transmissions
- S'appuie sur AES
- Propose un chiffrement des transmissions pour 802.11a, b et g.

802.11IR

- Infra rouges

802.11j

- Version japonaise de 802.11h