

Administration Système et Réseaux, Sécurité

WiFi

Philippe Harrand

¹Département Informatique
Pôle Sciences et Technologies

²Direction Territoriale Sud Ouest
France Télécom

4 décembre 2007

Wireless Fidelity

Modèle

Couche Physique

Couche Liaison de données

Sécurité

Mise en oeuvre

Intégration dans le modèle

- ▶ WiFi ⇒ couches 1 et 2
- ▶ Interface semblable à Ethernet
- ▶ Norme 802.11 **a, b ou g**

Intégration dans le modèle

| | | | | | |
|----------------------------|-----------------|------------------|-------------|----------------------|--------------|
| 802.2 Logical Link Control | | | | Media Access Control | Couche 2 OSI |
| 802.3 ethernet | 802.4 token bus | 802.5 token ring | 802.11 WIFI | | Physique |

A, B ou G ?

| Type | Débit | Fréquences | Canaux |
|---------|----------------------------|------------|--------|
| 802.11a | 54Mbit/s (30 Mb/s réels ?) | 5 GHz | 8 |
| 802.11b | 11Mbit/s (6 Mb/s réels ?) | 2,4 GHz | 3 |
| 802.11g | 54Mbit/s (30 Mb/s réels ?) | 2,4 GHz | 14 |

Puissance :

- ▶ intérieur 100 mW
- ▶ extérieur 10 mW

Portée :

- ▶ intérieur 10 à 60 m
- ▶ extérieur 300 m

Sensibilité : -80 db

Affaiblissement

| Matériau | Niveau d'atténuation |
|-----------------------------------|----------------------|
| Vitre épaisse non fumée | 1-2 dB |
| Placage/porte en bois | 2-3 dB |
| Cloison en plâtre | 3-5 dB |
| Box de bureau | 3-5 dB |
| Cloison en verre | 6 dB |
| Eau (bouteille/fontaine/aquarium) | 6-8 dB |
| Mur en brique | 8 dB |
| Tuiles en céramiques | 6-10 dB |
| Papier entreposé | 10 dB |
| Verre Blindé | 10-15 dB |
| Mur en béton | 10-15 dB |
| Miroirs/habillages métalliques | Reflexion Totale |

Signal

Interférences plus nocives que l'affaiblissement ⇒ codage

- ▶ Transmission d'une séquence de bits
- ▶ Barker Sequence (11 bits) pour un bit
- ▶ CCK (64 bits) pour 4 ou 8 bits

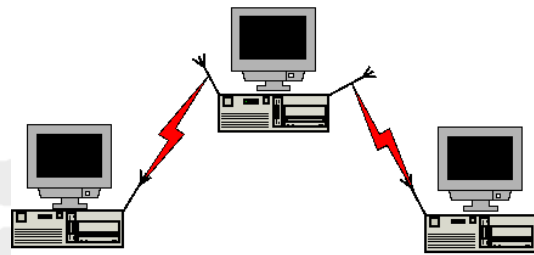
Modulation

- ▶ **OFDM** Orthogonal Frequency Division Multiplexing, Multiplexage par division en fréquences orthogonales
- ▶ **QPSK** Quadrature Phase Shift Keying. Saut de phase de 90°

Modes

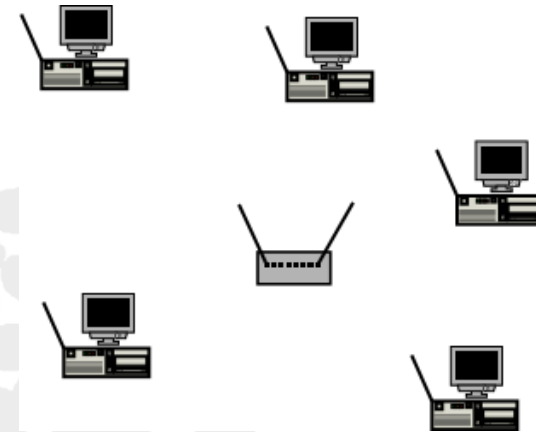
- ▶ Point à point
 - ▶ Ad Hoc
 - ▶ 2 stations
 - ▶ protocole de routage spécifique si plus de 2 stations
- ▶ Géré
 - ▶ Managed
 - ▶ 1 à N point d'accès
 - ▶ N stations
 - ▶ Accès contrôlé par l'AP
- ▶ Point d'accès
 - ▶ AP
 - ▶ BSS (Basic Service Set)
 - ▶ ESS (Extended Service Set)

Ad Hoc

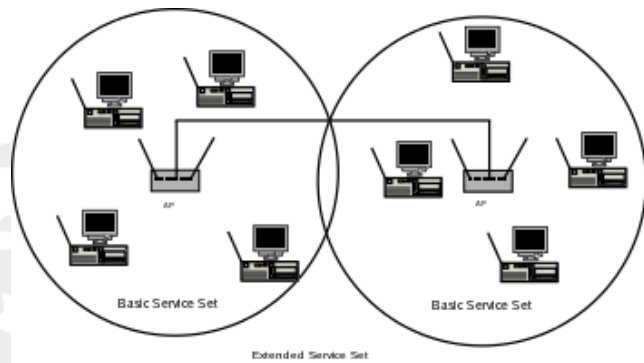


Mode Ad Hoc

BSS



ESS



Débit

- ▶ Débit variable suivant qualité du signal
- ▶ Une station éloignée ralentit tout le réseau
- ▶ Interfaces 802.11g compatibles avec 802.11b
- ▶ 108 Mb/s \Rightarrow 54Mb/s + compression

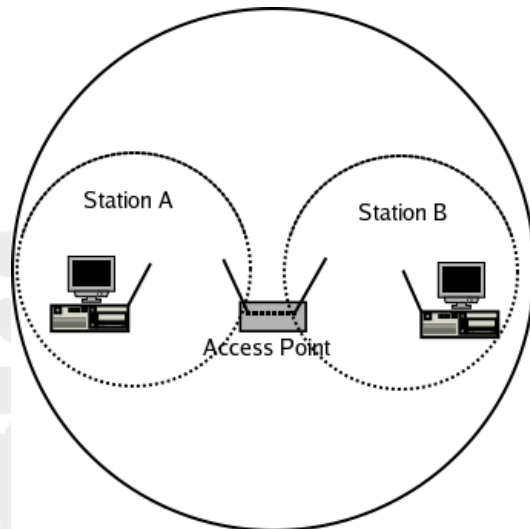
Accès au support

- ▶ **SIFS**, Short Inter Frame Space ($10\mu\text{spour}802.11g$)
- ▶ Possibilité de fragmentation au niveau **MAC**
- ▶ **DCF** (Distributed Coordination Function) \Leftrightarrow CSMA/CA
- ▶ **PCF** (Point Coordination Function)
- ▶ **VCF** (Virtual Carrier Sense) *RTS/CTS*

DCF (standard)

1. La station souhaitant émettre écoute
2. Si aucune transmission n'est détectée pendant un temps appelé DIFS, Distributed IFS ($28\mu\text{spour}802.11g$)
3. la station émet sa trame
4. L'entête de la trame contient la durée de la trame
5. Si la trame est reçue correctement (vérifié par le CRC), le récepteur envoie un accusé de réception ACK.
6. Si l'ACK n'est pas reçu par la station émettrice, la trame est considérée comme perdue et réémise après un temps aléatoire

Station cachée



PCF

- ▶ contrôlé par le point d'accès
- ▶ L'AP utilise un IFS plus court que les stations (**DIFS**)
- ▶ Temps est partagé entre périodes DCF et périodes PCF
- ▶ L'AP interroge chaque station à tour de rôle
- ▶ Aucune autre station ne peut émettre tant qu'elle n'a pas été interrogée
- ▶ Contrôle des collisions inutile

VCS

1. Émettre une trame Request To Send contenant l'adresse source, l'adresse destination et la durée de la transaction
2. Si la voie est libre, la station de destination (l'AP) envoie une trame Clear To Send qui contient les mêmes données
 - ▶ Trames RTS/CTS très courtes ⇒ peu de collisions
 - ▶ Charge du réseau est augmentée
 - ▶ Utilisé uniquement pour la transmission de trames longues

Association

- ▶ 2 stations doivent être associées
- ▶ Mode Managed
 - ▶ Requête d'association vers **AP**
 - ▶ éventuellement chiffrée
 - ▶ Contenant *ESSID*, débit, sur chaque canal
 - ▶ Les **AP** répondent
 - ▶ La station choisit le meilleur signal
- ▶ Les AP peuvent émettre leur *ESSID* (trame *BEACON*) en clair

Problématique

- ▶ L'accès à Ethernet nécessite une prise
- ▶ Pas de prises RJ45 sur un parking
- ▶ Les ondes hertziennes traversent les murs...

Sécurisation

- ▶ Les AP peuvent **NE PAS** émettre leur *ESSID*
- ▶ Les **ACL**
 - ▶ Interdisent l'association des hôtes indésirables
 - ▶ N'empêchent PAS d'écouter le trafic
 - ▶ Sécurité illusoire
- ▶ Chiffrement
 - ▶ **WEP**
 - ▶ WPA Personnel
 - ▶ WPA entreprise

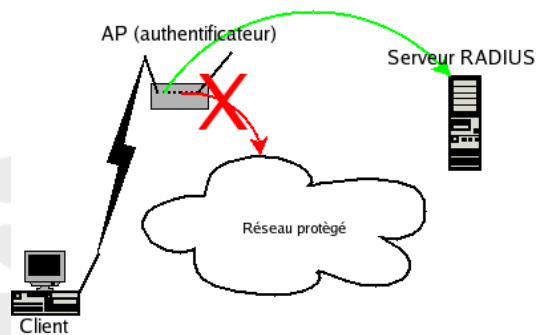
WEP

- ▶ ~~Wired Equivalent Privacy~~
- ▶ Chiffrement RC4 désormais faible
- ▶ Clef statique
- ▶ 64 (40) bits
- ▶ 128 (104) bits
- ▶ 100000 IV uniques suffisent pour le casser
- ▶ Que les logiciels actuels savent générer en 10mn
- ▶ A réserver à une utilisation familiale (et encore...)

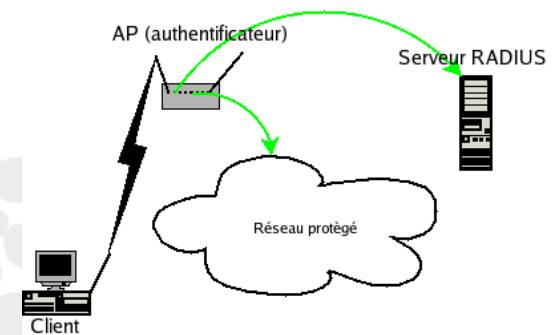
WPA

- ▶ **Wi-Fi Protected Access**
- ▶ 802.11i
- ▶ Clef générée dynamiquement avec **TKIP**
 - ▶ Changement de clef tout les 10 Ko échangés
 - ▶ Clef de 128 bits
 - ▶ Vecteur d'Initialisation de 48 bits
 - ▶ le VI change avec la clef
 - ▶ Contrôle d'intégrité sur tout le message
- ▶ **WPA PSK (Pre Shared Key)**
 - ▶ Clef générée dynamiquement à partir du mot de passe partagé
 - ▶ Mot de passe commun à toutes les stations
 - ▶ La longueur du mot de passe doit être supérieure à 20 octets
- ▶ **WPA Enterprise**
 - ▶ Serveur d'authentification RADIUS (Remote Authentication Dial-in User Service)

WPA EAP



WPA EAP



Windows

- ▶ Installez le logiciel fourni avec l'interface
- ▶ Affichez les connexions disponibles
- ▶ Cliquez sur le réseau choisi puis sur connecter
- ▶ Tapez 2 fois la clefs partagée
- ▶ Vous pouvez paramétrer plus finement avec "Modifier les paramètres avancés"

Linux

- ▶ Peu de drivers pour Linux mais le noyau (>2.6.17) contient un driver générique
- ▶ Les constructeurs n'en fournissent pas mais fournissent un *firmware* non libre
- ▶ Drivers développés par la communauté
- ▶ Les circuits Wifi évoluent très vite
- ▶ Ndiswrapper

Quelle interface ?

- ▶ lspci
- ▶ lspci -n
- ▶ Chercher sur le Net

Driver Linux

- ▶ Télécharger la toute dernière version
- ▶ Eventuellement cvs
- ▶ S'assurer que les fichiers entête du noyau en cours sont présents
- ▶ Compiler / installer
- ▶ Parfois récupérer le *firmware* non libre de l'interface
- ▶ **RTFM**

Ndiswrapper

- ▶ Paquetages binaires ou télécharger / compiler la toute dernière version
- ▶ Chercher sur le wiki de ndiswrapper le driver Windows qui va bien
- ▶ ndiswrapper -i pour installer le driver
- ▶ ndiswrapper -l pour vérifier que (peut-être) ça marche
- ▶ modprobe ndiswrapper pour charger de driver

Wireless Tools

- ▶ iwlist scan ⇒ réseaux disponibles
- ▶ iwconfig sans paramètres ⇒ état des interfaces Wifi
- ▶ iwconfig avec paramètres ⇒ associer l'interface avec une autre
- ▶ iwconfig avec paramètres ⇒ configuration de l'interface
- ▶ iwconfig avec paramètres ne renvoie jamais rien
- ▶ iwpriv ⇒ configuration de paramètres spécifiques
- ▶ Après association ⇒ comme ethernet

WPA

- ▶ wpa_passphrase ⇒ générer la clef partagée
- ▶ wpa_cli ⇒ commandes interactives *wpa_cli -h*
- ▶ wpa_supplicant ⇒ client wpa