M1 Informatique

Réseaux

Wi-Fi

Bureau S3-354
Mailto:Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M1/rezopro

Wi-Fi - Introduction

Le "Wi-Fi" correspond à un ensemble de normes IEEE de la famille 802.11 (Ethernet = 802.2).

Il s'agit d'une technologie de réseau avec la couche physique adaptée.

Ses particularités impliquent des mécanismes de sécurité appropriés (norme 802.11i notamment)

Wi-Fi - Historique

Première connexion sans fil entre ordinateurs : 1970 !
(relié au réseau Arpanet)
Mais : faible débit (quelques Kbs/s)

Débit tjs inférieur au filaire, mais exploitable (~10 Mbs/s)

Retards dûs également à la normalisation, à la réglementation : fin 2002 : utilisation possible de la bande des 2,4 Ghz.
Normalisation "Wi-Fi" : 1998-1999

Wi-Fi - Performances

Débits théoriques :

802.11b : 11 Mb/s
802.11g : 54 Mb/s
802.11n : débit théorique de plusieurs centaines de Mb/s

En pratique, diviser ces valeurs par 2 au moins (voir plus loin les techniques utilisées)

Wi-Fi - Utilité

Pas (ou peu) de câblage :

Réseau domestique
Extension de réseaux d'entreprise (salles de réunion, bâtiments anciens non câblés, ...)
Points d'accès dans lieux publics (gares, aéroports, ...)
Antennes d'accès libre à l'initiative de particuliers ou associations

Wi-Fi - Fréquences

La bande de fréquence utilisée est celle de 2,4 Ghz
Il y a en fait 14 "canaux" dans cette bande, de 2,412 à 2,477 Ghz (donc distants de 5Mhz).
Le 802.11a, et maintenant le n, utilisent la bande de 5Ghz

La transmission aux vitesses annoncées nécessite toutefois des bandes plus larges (25 Mhz). Dans un même réseau, on utilisera des canaux distants (1, 6 et 11 par exemple)

Wi-Fi – Disposition des bornes

Pour couvrir un bâtiment, il faut en général plusieurs bornes (portée du Wi-Fi assez faible, obstacles, ...)

Les zones couvertes par les différentes bornes se recouvrent partiellement. Il faut alors utiliser des canaux différents pour des bornes voisines.

Il est donc nécessaire de disposer les bornes et choisir les canaux

Wi-Fi - Technologie

FHSS : saut de fréquence :
(Frequency Hopping Spread Spectrum)
on utilise successivement des bandes de fréquences différentes, distantes de 1Mhz.
Origine : applications militaires : avec séquence secrète.

Le changement de bande est fréquent : toutes les demi-secondes environ

On utilise à présent ce mécanisme avec une séquence connue (publique). Le but est d'éviter les interférences.

Wi-Fi - Technologie

DSSS : étalement de fréquence :
(Direct Sequence Spread Spectrum)
1 bit représenté par une séquence connue de bits
la variation est plus rapide, donc nécessité d'une bande de fréquence plus large, donc limitation (~ 1Mb/s).

Mais, avec plusieurs séquences connues, possibilité d'augmenter le débit (la séquence "transporte" des bits supplémentaires : 8 bits => 11Mb/s)

Wi-Fi - Technologie

Des techniques plus évoluées permettent d'utiliser des fréquences voisines (donc se chevauchant) mais sans interférences grâce aux choix judicieux des fréquences : fréquences « orthogonales » **OFDM (Orthogonal Frequency Division Multiplexing)**

Ceci permet d'obtenir des débits plus importants : 54 Mb/s pour le 802.11g par exemple.

==> jusqu'à 500 Mb/s (802.11n) en utilisant plusieurs techniques conjuguées.
Le 80.11n utilise également plusieurs antennes, éventuellement la bande 5Ghz.

Wi-Fi – Trame 802.11

Se compose de :

- un préambule
- une en-tête
- la partie utile

Le préambule permet une synchronisation (nécessaire en FHSS comme en DSSS). Il y a les versions "courts" et "longs"

L'en-tête fixe la longueur de la partie utile, le débit et comporte une séquence de contrôle

Wi-Fi – Couche MAC

Cette sous-couche définit :

- le format de la trame
- le protocole de communication entre les équipements
- les mécanismes de contrôle et de partage de la bande passante
- les mécanismes de sécurité

Wi-Fi – CSMA / CA

La détection de collision ne peut pas fonctionner comme pour Ethernet (les stations peuvent ne pas se "voir").

Il faut donc un mécanisme pour éviter ces collisions.

CSMA / CA : les trames doivent être acquittées, et un mécanisme complémentaire gère le tour de parole (en mode infrastructure)

Wi-Fi – Mode DCF

Distributed coordination function
Une station qui désire émettre :

- attend un temps de silence minimal + délai aléatoire
- envoie un petit paquet RTS (collision peu probable ici)
- reçoit un CTS si le correspondant est OK
- envoie ses données
- attend un acquittement

Le RTS précise le "temps de parole" demandé.
Les autres stations respectent ce temps de parole accordé à la station par le CTS

Wi-Fi – Pbs lié au DCF

Mécanisme valable seulement en unicast
Beaucoup de collisions évitées mais perte de performances
Pour les petits paquets de données, RTS et CTS n'apportent rien

Ce mécanisme n'est pas valable si les stations sont nombreuses

Wi-Fi – mode PCF

Point coordination function
Le point d'accès (AP) distribue la parole aux stations.

Il n'y a plus de collisions

l'AP accorde un temps de parole à chaque station. Si cette dernière en a besoin, elle émet un acquittement puis ses données.
Si elle n'a pas répondu dans un délai court, la parole est passée à une autre station

Wi-Fi – mode PCF (suite)

PCF peu efficace si la plupart des stations sont silencieuses.
En fait, on peut utiliser alternativement PCF / DCF
La séquence PCF / DCF est initialisée par l'émission (par l'AP) d'une "balise".
Cette dernière indique la durée de la phase PCF, qui peut éventuellement être raccourcie par l'émission d'un signal de fin de cette phase.
Les équipements actuels utilisent des versions améliorées de ces principes.

Wi-Fi – Mode Ad-Hoc

Constitution de réseaux "de poste à poste"
Un poste déclare un réseau, les autres (situés à proximité) l'utilisent.
Donc plusieurs postes possibles, mais pas de gestion de tour de parole

Risque de collisions si les postes sont trop nombreux.
Nécessité de configurer le niveau réseau (IP).

Utile pour quelques échanges de données dans une réunion par exemple.

Wi-Fi – Mode Infrastructure

Un ou plusieurs points d'accès gèrent les stations situées à proximité.
Ils font partie du même réseau, identifié par un "ssid"
Les fréquences doivent être correctement réparties pour éviter les interférences dans les zones de recouvrement

Chaque AP définit un "Basic Set service" identifié par son "bssid" égal à son adresse MAC

L'ensemble des AP définit un "Extended Set service" identifié par son "essid" ou simplement "ssid"

Wi-Fi – Association

En mode infrastructure, les balises donnent des infos : Bssid, débits disponibles, éventuellement ssid.
Une station peut également essayer de détecter un réseau dont elle connaît le ssid

Une station envoie une requête d'identification au réseau dont elle choisit le ssid (reçu ou connu).

Selon le niveau de sécurité, la connexion est acceptée ou nécessite une identification plus ou moins poussée.

Wi-Fi – Sécurité

L'AP peut reconnaître l'adresse MAC de la station. Ce n'est pas très sûr, on peut facilement usurper cette adresse.
La clef Wep peut être sollicitée pour authentifier la station.
Mais, là encore, ceci peut être contourné :
- soit par une attaque "Man in the Middle", un pirate interceptant toutes les communications, puis se faisant passer pour la station
- soit avec un programme de décodage, après écoute d'un certain nombre d'échanges.
Le WPA est plus sûr... mais toutefois pas inviolable.

Wi-Fi – économie d'énergie

Une station peut se mettre en sommeil lorsqu'elle n'a plus rien à envoyer.
Des bits des paquets permettent de prévenir le correspondant qu'on va se mettre dans ce mode, ou au contraire qu'on a encore des données à envoyer.

L'AP met en file d'attente les paquets destinés à une station en sommeil, et envoie dans les balises la liste des stations pour lesquelles elle a des paquets.
Les stations doivent se reveiller périodiquement, recevoir ces balises et savent donc qu'elles ont des données à recevoir

Wi-Fi – En-têtes

Par rapport aux trames Ethernet, les trames Wi-Fi ont des informations supplémentaires :

- Deux bits "fromDS" et "toDS" indiquent si l'émetteur (resp. le destinataire) appartient au système de distribution (i.e. est un AP).
- La trame peut véhiculer jusqu'à quatre adresses Mac, en fonction des valeurs de ces deux bits (voir tableau page suivante)

Wi-Fi – @Mac

ToDS	FromDS	Addr1	Addr2	Addr3	Addr4
0	0	Dest	Source	BSSID	0
1	0	AP	Source	Dest	0
0	1	Dest	AP	Source	0
1	1	Ap suiv.	AP	Dest	Source

Wi-Fi : paquets

Le paquet Wi-Fi contient les champs suivants :

FC (2 octets) voir page suivante
D/ID (2 octets) temps d'émission du paquet (ou ID station pour paquets Poll)
Adr1, Adr2, Adr3, Adr4 (6 octets chaque)
SC (2 octets) gère la fragmentation
Données (jusqu'à 2312 octets)
FCS (4 octets) séquence de contrôle

Wi-Fi : champ FC

Le détail du champ FC est le suivant :

Version : 2 bits
Type (2 bits) et sous-type (4 bits)
(paquets gestion, contrôle ou données)
Bits toDS et FromDS
Bits Frag, Retry, Sleep, More
Bit Wep, Bit Order