Réseaux sans-fil et réseaux de mobiles

Florent Dupont
fdupont@liris.cnrs.fr
http://liris.cnrs.fr/florent.dupont

Objectifs du cours

- Comprendre les spécificités des réseaux "sans-fil" dans la transmission, depuis les couches basses jusqu'aux applications
- Étudier les exemples de technologies actuelles pour illustrer :
  - les notions d'architecture (station de base, cellule…)
  - les mécanismes de handover
  - les problèmes de sécurité
  - etc.

➢ Enjeu économique et social : très forte croissance, modification des comportements humains (travail, loisir, communication, etc.)

Documents, bibliographie

- **Réseaux de mobiles et réseaux sans fil**
  Al Agha, Pujolle, Vivier (Eyrolles)
- **802.11 et les réseaux sans fil**
  *Paul Muhlethaler (*Eyrolles)
- **Principles of Wireless Networks**
  *K. Pahlavan, P. Krishnamurthy (*Prentice Hall)
- **Wi-Fi par la pratique**
  *Davor Males et Guy Pujolle (*Eyrolles)
- ***ART – Autorité de Régulation des Télécommunications***
  http://www.art-telecom.fr/

+ nombreux sites…

Plan du cours (1)

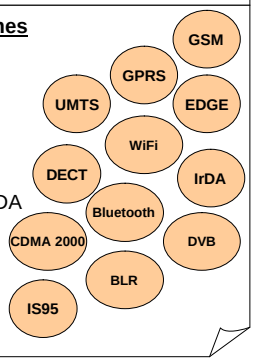
1ère partie

- Historique
- Utilisation des bandes de fréquences
- Rappels : Bases de la transmission
- Propagation
- Principes fondamentaux spécifiques :
  - Mobile,
  - Antenne,
  - Architecture,
  - Cellule,
  - Handover
  - etc.

Plan du cours (2)

2ème partie : exemples de systèmes

- GSM - GPRS/EDGE - UMTS
- WiFi
- Systèmes satellites : TV, WiFi
- DVB
- Boucle Radio Locale
- Systèmes : DECT, Bluetooth, IrDA
- Systèmes IS95, CDMA 2000
- IP Mobile
- Services mobiles
- Réseaux futurs : 4G



Historique

Historique

- 1838 : Théorie (S. Morse)
- 1858 : Câble transatlantique
- 1864 : Équations de Maxwell
- 1865 : Télégraphe (S. Morse)
- 1876 : Téléphone (Bell)
- 1898 : 1ère communication mobile (Marconi, puis Armée US)
- 1915 : 1ère liaison téléphonique transcontinentale (Bell System)
- 1930 : Télévision (principes)

Historique

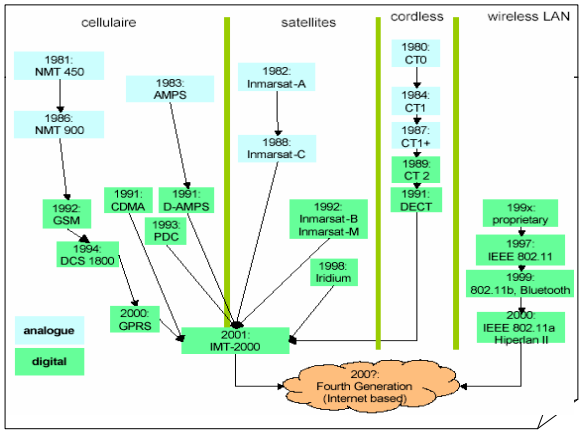
- 1948 : Invention du transistor, théorie de Shannon
- 1950 : nombreuses communications mobiles professionnelles
- 1958 : 1er réseau cellulaire public (Allemagne)
- 1962 : 1er satellite TV (Telsar I)
- 1962 : 1er satellite géostationnaire (Intelsat I)
- 1964 : Transmission de données sur RTC
- 1969 : Internet
- 1970 : Bell / 1G

Historique

- 1970 : début des systèmes cellulaires analogiques
- 1980 : début des systèmes sans cordon
- 1983 : Études GSM (numérique)
- 1985 : Études DECT
- 1988 : Débuts GSM / Études CDMA
- 1990 : IEEE 802.11 Wireless LAN
- 1990 : Messagerie unilatérale (étape)
- 1991 : Déploiement GSM
- 1993 : DEC 1800, début IS-95 (CDMA)

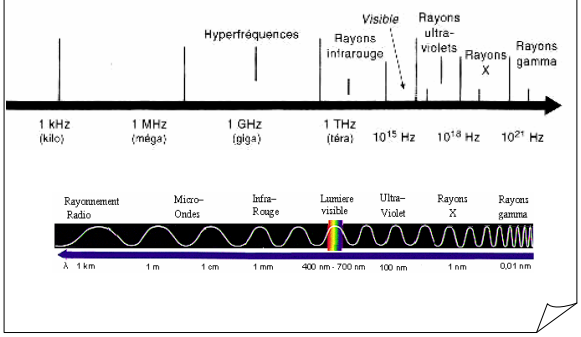
Développement du sans-fil

- La déréglementation a joué un rôle important…
- Progrès en électronique :
  - miniaturisation des équipements
  - augmentation de l'autonomie (batteries)
  - réduction du prix des équipements
- Moyen le plus rapide et le moins coûteux pour couvrir un territoire sans "re-câbler"
- Intérêt de la mobilité
  - ne pas confondre sans-fil et mobile

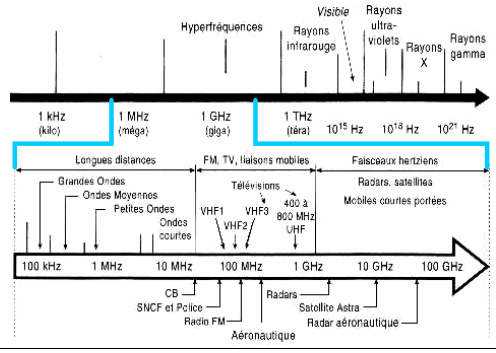


Utilisation des bandes de fréquences

Utilisation des bandes de fréquences



Utilisation des bandes de fréquences



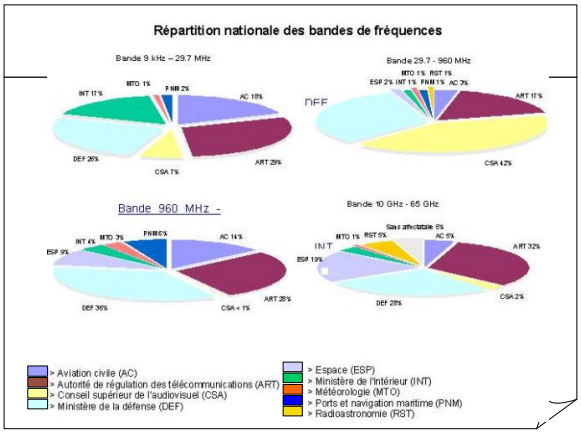
Agence nationale des fréquences (www.afnr.fr)

- **Bandes de fréquences** : attribuées aux différents services de radiocommunication par le ***Règlement des radiocommunications*** de **l'Union internationale des télécommunications**, élaboré par les conférences mondiales des radiocommunications.
- **En France, les bandes ainsi attribuées sont réparties entre 9 affectataires (7 administrations et 2 autorités indépendantes)**
  - **AC** Administration de l'aviation civile
  - **DEF** Ministère de la défense
  - **ESP** Espace
  - **INT** Ministère de l'intérieur
  - **MTO** Administration de la météorologie
  - **PNM** Administration des ports et de la navigation maritime (ex phares et balises)
  - **RST** Ministère de l'éducation nationale, de la recherche et de la technologie
  - **CSA** Conseil supérieur de l'audiovisuel
  - **ART** Autorité de régulation des Télécommunications

Agence nationale des fréquences (www.afnr.fr)

- + des fréquences utilisables pour certains matériels de faible puissance et de faible portée
- Exemple :

Bande des fréquences	2400 à 2454 MHz
Puissance max.	100 mW
Largeur canal	non imposée
Références	Décisions ART N°xxx



Rappels : Bases de la transmission

Fréquences : Fourier

- Toute **fonction périodique g(t)** ayant pour période **T=1/f** peut se décomposer en une somme de fonctions périodiques sinusoïdales et cosinusoïdales :

$$g(t) = c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} b_n \cos(2\pi nft)$$

- Les coefficients a_n et b_n sont les amplitudes respectives des sinus et cosinus (harmoniques) et c est égal à la valeur moyenne du signal :

$$a_n = \frac{2}{T}\int_0^T g(t)\sin(2\pi nft)dt, \quad b_n = \frac{2}{T}\int_0^T g(t)\cos(2\pi nft)dt, \quad c = \frac{1}{T}\int_0^T g(t)dt$$

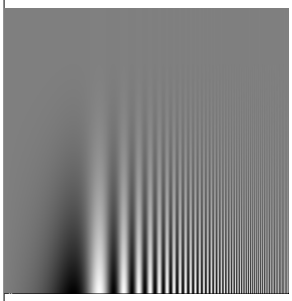
- Cette décomposition est appelée ***série de Fourier***.
- Exemples : fréquences dans un signal, une image…

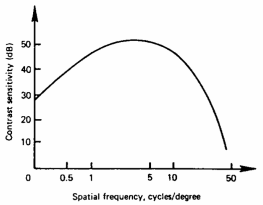
Fréquences : Fourier

- **Transformée de Fourier**
  → Représentation d'un signal sur une base de fonctions exponentielles complexes
  – Cas mono-dimensionnel

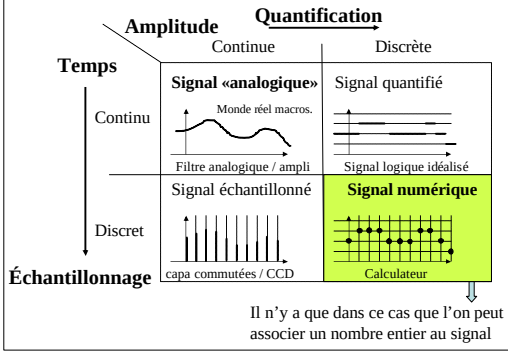
$$f(x) = \int_{-\infty}^{+\infty} F(u).e^{2\pi jux}\,du \qquad \underset{F^{-1}}{\overset{F}{\rightleftarrows}} \qquad F(u) = \int_{-\infty}^{+\infty} f(x).e^{-2\pi jux}\,dx$$

Exemple : réponse en fréquence de l'oeil





Numérisation / discrétisation

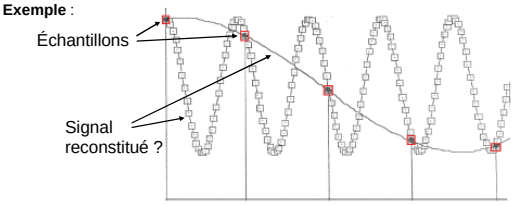


Il n'y a que dans ce cas que l'on peut associer un nombre entier au signal

Échantillonnage : Théorème de Shannon

Théorème De Shannon: Fe > 2 x Fmax(Signal)

Exemple :



Un signal incorrectement échantillonné ne pourra pas être reconstitué

Bande passante

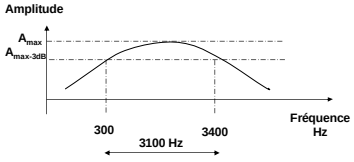
La **bande passante** caractérise tout support de transmission, c'est la bande de fréquences dans laquelle les signaux sont correctement reçus :

W = Fmax – Fmin (en Hz)

➢ Le spectre du signal à transmettre (éventuellement modulé) doit être compris dans la bande passante du support physique.

Bande passante

- Exemples:
- l'atmosphère élimine les U.V.
- l'oreille humaine est sensible dans la bande 20 Hz-20 KHz
- Réseau téléphonique commuté (RTC)



Débit maximum d'un canal de transmission

- Si un signal quelconque est appliqué à l'entrée d'un filtre passe-bas ayant une bande passante W, le signal ainsi filtré peut être reconstitué avec un échantillonnage à 2W/s (Nyquist, Shannon)

$$D_{max} = 2\ W \log_2 V \quad \text{en bit/s}$$

si le signal comporte V niveaux significatifs (Valence).

➢ La bande passante limite la **rapidité de modulation**.

Exemple: Pour un canal sans bruit dont la bande passante est de 3000 Hz qui ne peut transmettre qu'un signal binaire, D max = 6000 bit/s.

Bruit, capacité

- Bruits aléatoires ⇒ dégradation de la transmission
- Quantité de bruit = rapport de la puissance du signal transmis à la puissance du bruit

  = rapport signal sur bruit, (SNR en anglais signal to noise ratio ou **S/N**).
- Pour un canal de transmission de bande passante W perturbé par du bruit dont le rapport signal sur bruit est S/N, la **capacité** de transmission maximale C en bit/s vaut :

$$C = W \log_2 (1+P_S/P_N) \quad \text{en bit/s}$$

S/N est exprimé en dB en général, mais pas dans la formule !

$$(S/N)_{dB} = 10 \log_{10} (P_S/P_N) \Leftrightarrow P_S/P_N = 10^{(S/N)_{dB}/10}$$

- **Exemple**: Pour un canal dont la bande passante est de 3000 Hz et un rapport S/N=30dB, (valeur typique du réseau téléphonique analogique), P_S/P_N=1000 => C = 30 000 bit/s.

Perturbations

- Perturbations ⇒ l'information extraite du signal reçu peut conduire à des erreurs.
- Causes multiples, principale préoccupation dans les systèmes de télécommunication.
- **Affaiblissement ou atténuation = perte d'énergie du signal pendant sa propagation**

$$\text{Atténuation (dB)} = 10 \log_{10} (P_1/P_2)$$

(-3 dB correspond à une perte de la moitié de la puissance)

- Affaiblissements différents suivant les harmoniques ⇒ **distorsions**

  En pratique affaiblissements d'amplitude négligeable jusqu'à f_c appelée ***fréquence de coupure***.

  Pour compenser cet affaiblissement et pour permettre des transmissions sur de longues distances ⇒ amplificateurs ou répéteurs

Perturbations

- L'atténuation augmente avec la fréquence (passe-bas).
- La **distorsion temporelle** = toutes les composantes harmoniques d'un signal ne se propagent pas à la même vitesse.
- Un **déphasage** du signal (distorsion de phase) constitue une perturbation. $\Phi = \Phi(f)$. Le déphasage dépend de la fréquence. Le temps de groupe est donné par :

$$T(f) = \frac{1}{2\pi} \times \frac{d(\Phi(f))}{df}$$

Bruit

- Tout signal indésirable interprété par le récepteur et délivrant une information incohérente.
- **Sources de bruit** :
  - émetteur du signal ;
  - media de transmission ;
  - perturbation atmosphérique.
- **Bruit thermique** = agitation thermique des électrons (source de bruit la plus courante)
- **Diaphonie** = influence mutuelle entre deux signaux utiles mais sur des conducteurs voisins.

Modulation / Démodulation

- Transmission d'un signal à spectre étroit sur un support à large bande passante ⇒ mauvaise utilisation du support

⇒ techniques de **modulation** et de **multiplexage**

- Soit un **signal périodique** : $y(t) = A \sin(2\pi ft + \Phi)$
- Signal transporté sous forme d'une onde faisant varier une des caractéristiques physiques du support:
  - différence de potentiel électrique;
  - onde radioélectrique
  - intensité lumineuse

Porteuse: $p(t) = A_p \cos(2\pi f_p t + \Phi_p)$

- On fait ensuite subir des déformations ou modulations à cette porteuse pour distinguer les éléments du message.

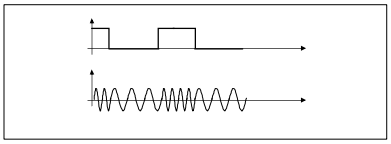
Modulation

- ***La modulation est la transformation d'un message à transmettre en un signal adapté à la transmission sur un support physique.***
- Les objectifs de la modulation sont:
  - une transposition dans un domaine de fréquences adapté au support de transmission;
  - une meilleure protection du signal contre le bruit;
  - une transmission simultanée de messages dans les bandes de fréquences adjacentes, pour une meilleure utilisation du support.
- Trois types de modulation de base existent, en faisant varier les trois paramètres de l'onde porteuse: A_p, f_p, Φ_p.

Modulation de fréquence

(FSK: Frequency Shift Keying)

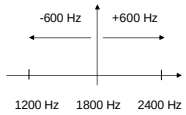
- une valeur de fréquence ↔ une valeur du signal



Modulation de fréquence

- Porteuse sinusoïdale de fréquence F_0 modulée par deux fréquences opposées $+f_0$ et $-f_0$

⇒ une fréquence est associée à chaque niveau logique.



Modulation de fréquence

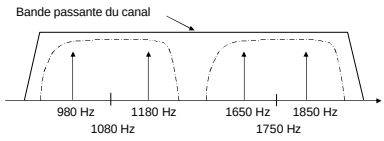
- Liaison "full-duplex":

Émission / Réception simultanée

⇒ on partage la bande passante du canal

une voie à l'émission F_1 +/- f_1

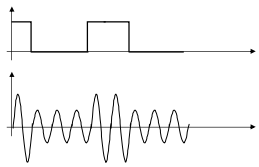
+ une voie à la réception F_2 +/- f_2



Modulation d'amplitude

(ASK: Amplitude Shift Keying)

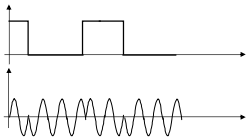
- une valeur d'amplitude ↔ une valeur du signal



Modulation de phase

(PSK: Phase Shift Keying)

- un déphasage ↔ une valeur du signal

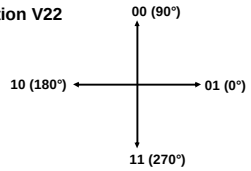


- Avec des codes à plusieurs bits, on peut augmenter le débit sans changer la fréquence de modulation.
- Les vitesses de transmission sont plus élevées qu'en modulation FSK pour la même bande passante

Modulation de phase

- Exemple : avis V22 du CCITT (1200 bauds) - phase codée sur 2 bits

Constellation V22



➢ Nombre de déphasages limité par le bruit pour retrouver le bon signal

Modulation combinée

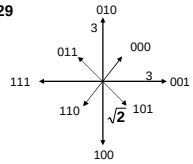
- Combiner plusieurs types de modulation parmi les trois types de modulation décrits auparavant.

➢ Les normes actuelles utilisent des combinaisons des modulations de phase et d'amplitude.

Exemple : Modulation V29 à 7200 bits/s

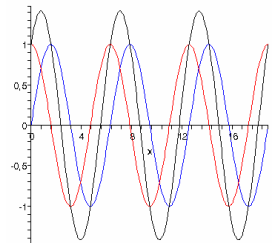
- 8 états de phase et 2 valeurs d'amplitude

Constellation V29



Modulation combinée en quadrature

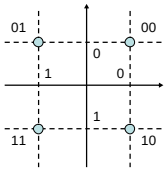
- Porteuses en quadrature : addition de deux porteuses de fréquence f_0 en quadrature, on obtient une seule porteuse, toujours de fréquence f_0



Modulation combinée en quadrature

Modulation de phase

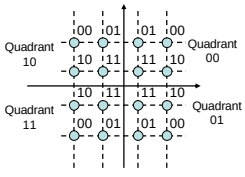
4 états (2 bits)



Quadrature Amplitude Modulation

QAM 16

16 états (4 bits)



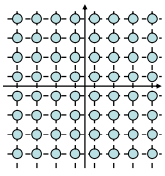
Modulation des 2 porteuses

Modulation combinée en quadrature

Quadrature Amplitude Modulation

QAM 64

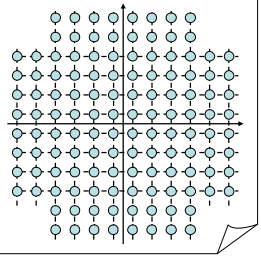
64 états (6 bits)



Quadrature Amplitude Modulation

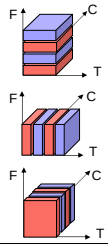
QAM 128

128 états (7 bits)



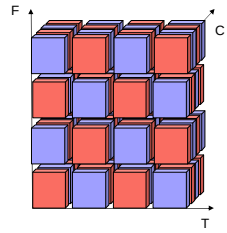
Multiplexage

- **Objectif** : optimiser l'usage des canaux de transmission pour un transit simultané du maximum d'informations ⇒ **partage** (**multiplexage**) du support physique de transmission entre plusieurs signaux.
- Ces techniques peuvent se classer en trois grandes catégories:
  - **multiplexage fréquentiel** :
    MRF (Multiplexage par Répartition de Fréquence)
    FDM (Frequency Division Multiplexing)
  - **multiplexage temporel** :
    MRT (Multiplexage à Répartition dans le Temps)
    TDM (Time Division Multiplexing)
  - **multiplexage par code**
    CDM (Code Division Multiplexing)



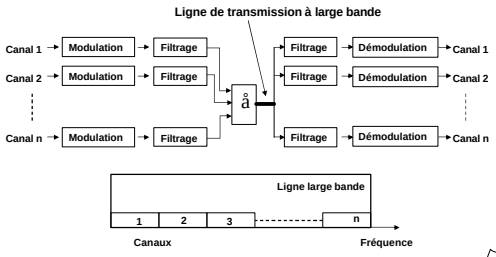
Multiplexage

- La réalité est parfois (?) plus complexe…



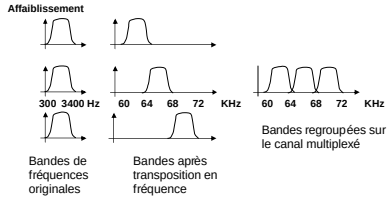
Multiplexage en fréquences

- **Partage de la bande de fréquences** disponible en plusieurs canaux (ou sous-bandes) plus étroits : en permanence chacun de ces canaux est affecté à un "utilisateur" exclusif



Multiplexage fréquentiel de trois canaux téléphoniques

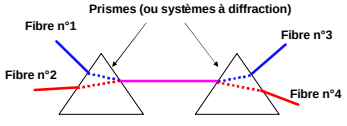
- **3 liaisons téléphoniques multiplexées avec technique FDM.**
- Des filtres appropriés limitent la bande passante à 3100 Hz par canal téléphonique.
- Pour assurer un multiplexage correct, une bande de fréquences de 4000 Hz est attribuée à chaque canal afin de bien les séparer les uns des autres.



Multiplexage en longueur d'onde

WDM (Wavelength Division Multiplexing)

⇒ proche du multiplexage fréquentiel



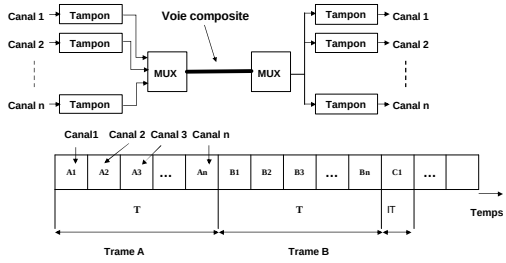
- Entrée : 2 fibres : flux lumineux d'énergie et de bande de fréquences différentes

⇒ Multiplexage WDM complètement passif ⇒ très haute fiabilité.

- Fibre W ~ 25000 GHZ
- un signal: qq GHz (limite = pb de conversion lumière/électricité)

Multiplexage temporel

⇒ chaque "utilisateur" a pendant un court instant et à tour de rôle, la totalité de la bande passante disponible (généralement réservé aux signaux numériques).



Multiplexage temporel

- La vitesse de transmission des voies bas débit (*d*) est fonction de la vitesse de transmission de la ligne (*D*) et du nombre de voies *n*

  d=D/n

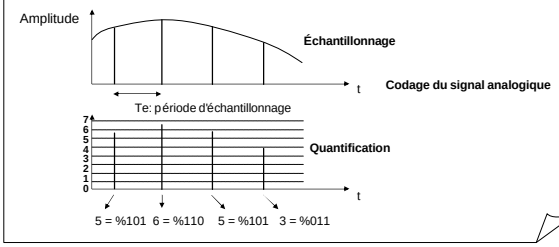
- La période *T* des trames est fonction du nombre de voies et de l'intervalle de temps élémentaire IT.

  T= n x IT

Modulation par impulsions codées (MIC)

Multiplexage temporel pour les transmissions téléphoniques.

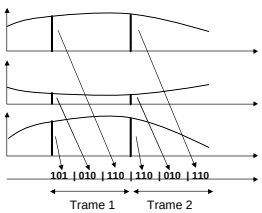
- échantillonnage des signaux analogiques de chacune des voies;
- quantification et codage des échantillons multiplexés pour obtenir un signal numérique.
- multiplexage temporel des échantillons des différentes voies;



Modulation par impulsions codées (MIC)

- Les échantillons sont ensuite multiplexés pour former un ensemble de trames.

Multiplexage temporel des échantillons de trois voies



Multiplexage temporel statistique

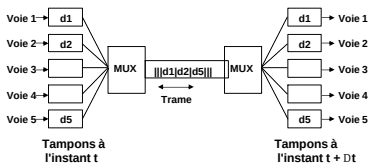
- Multiplexage temporel simple : tranches de temps pas toujours utilisées ⇒ des bits ou des caractères de remplissage sont insérés.
- Multiplexage temporel statistique ou asynchrone
  (ATDM: Asynchronous Time Division Multiplexing)
- **Allocation dynamique des tranches de temps aux seules voies qui ont des données à transmettre à un instant donné.**

⇒ permet de raccorder plusieurs équipements sur une seule ligne, même si le débit cumulé de chaque voie est supérieur au débit maximum de la ligne.

⇒ Le multiplexeur intègre un microprocesseur et des mémoires tampon:
il permet **des débits et des paramètres de transmission différents sur chaque voie** ou sous-canal et à chaque extrémité.

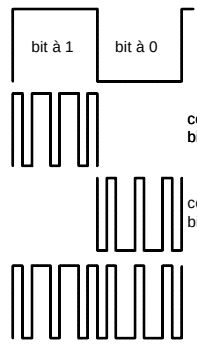
Multiplexage temporel statistique

- Le multiplexeur :
  - détecte les tampons non vides,
  - prélève les données mémorisées,
  - supprime les bits non significatifs dans le cas d'une transmission asynchrone (start, stop, parité),
  - comprime éventuellement les données et les insére dans les trames de la voie composite.



Étalement de spectre : DSSS

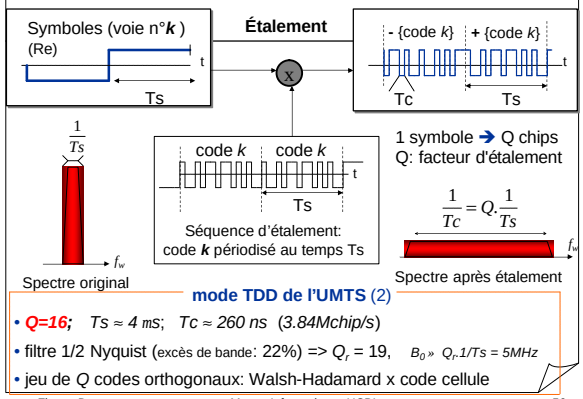
- Données à transmettre
- Code pseudo-aléatoire
  - Exemple avec 10 chips
- Signal de sortie



Étalement de spectre : Comparatif

Caractéristiques	Saut de Fréquence FHSS	Séquence directe DSSS
Avantages	La + sûre Env. difficile	La + employée Env. peu perturbé
Débit théorique (Mb/s)	1	2
Débit effectif (Mb/s)	0.3 à 0.7	1.2 à 1.4
Sécurité	Séquence de saut	Code d'étalement
Taux d'erreur moyen	10^{-3}	10^{-8}
Distance maximale en intérieur	50 m	25 m
Distance maximale en extérieur	800 m	200 m
Cohabitation entre WLAN	simple	contraignant
Nb max de stations par AP	30 à 50	10 à 20
Remarques	Partage de la bande passante	Média monopolisé par émetteur

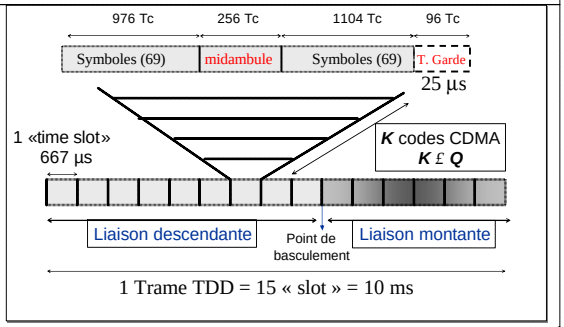
Principe du CDMA: étalement de spectre par les codes



mode TDD de l'UMTS (2)

- ***Q=16***; *Ts ≈ 4 ms*; *Tc ≈ 260 ns* (*3.84Mchip/s*)
- filtre 1/2 Nyquist (excès de bande: 22%) => Q_r = 19, $B_0 \gg Q_r \cdot 1/Ts = 5MHz$
- jeu de *Q* codes orthogonaux: Walsh-Hadamard x code cellule

Synoptique de la trame TDD-UMTS (Voie de données)



Propagation

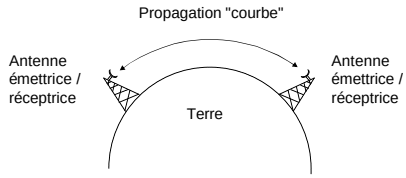
Gain d'antenne

- Relation entre le gain d'antenne et la surface effective de l'antenne :

$$G = \frac{4\pi A_e}{\lambda^2} = \frac{4\pi f A_e}{c^2}$$

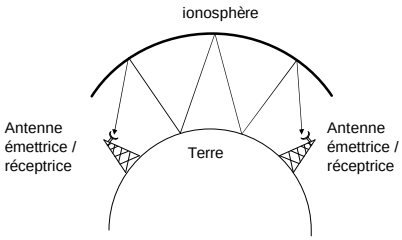
  - G = gain
  - A_e=surface effective
  - f = fréquence de la porteuse
  - c = vitesse de la lumière 3.10^8 m/s
  - ?= longueur d'onde de la porteuse

Propagation par onde de sol



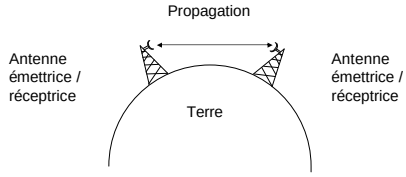
- Suit la courbure de la terre
- Grandes distances
- Fréquence -> 2 MHz
- Exemple Radio AM

Propagation ionosphérique



- Réflexion sur la ionosphère
- Grandes distances
- Fréquence -> 30 MHz

Ligne directe



- LOS (Line of Sight)
- Antennes d'émission et de réception en ligne directe
- La vitesse des ondes dépend du milieu traversé
- Le changement de milieu (indice de réfraction) induit une "courbure" dans le trajet

Atténuation

- Dépend essentiellement de la distance

$$P_r = P_e d^{-\alpha}$$

- avec :
  - P_e = puissance émise (antenne émission)
  - P_r = puissance reçue (antenne réception)
  - d = distance entre les antennes
  - a pouvant varier de 2 à 4

Atténuation

- Pour une antenne idéale isotropique :

$$\frac{P_e}{P_r} = \frac{(4\pi d)^2}{\lambda^2} = \frac{(4\pi f d)^2}{c^2}$$

  - P_e = puissance émise (antenne émission)
  - P_r = puissance reçue (antenne réception)
  - d = distance entre les antennes
  - c = vitesse de la lumière 3.10^8 m/s
  - ?= longueur d'onde de la porteuse

Pertes en dB

- Calcul en fonction de la fréquence et de la distance :

$$L_{(dB)} = 10\ log\left(\frac{P_e}{P_r}\right) = 20\ log\left(\frac{4\pi d}{\lambda}\right) = 20\ log\left(\frac{4\pi f d}{c}\right)$$

$$L_{(dB)} = 20\ log(f) + 20\ log(d) - 147{,}56\ dB$$

Pertes en dB

- Calcul en tenant compte des antennes :

$$\frac{P_e}{P_r} = \frac{(4\pi d)^2}{G_r G_e \lambda^2} = \frac{(\lambda d)^2}{A_r A_e} = \frac{(cd)^2}{f^2 A_r A_e}$$

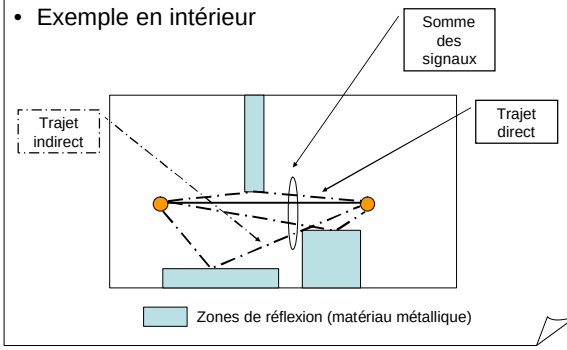
$$L_{(dB)} = 20\ log(\lambda) + 20\ log(d) - 10\ log(A_e A_r)$$

$$L_{(dB)} = -20\ log(f) + 20\ log(d) - 10\ log(A_e A_r) - 169{,}54\ dB$$

  - G_e = gain de l'antenne d'émission
  - G_r = gain de l'antenne de réception
  - A_e = surface effective de l'antenne d'émission
  - A_r = surface effective de l'antenne de réception

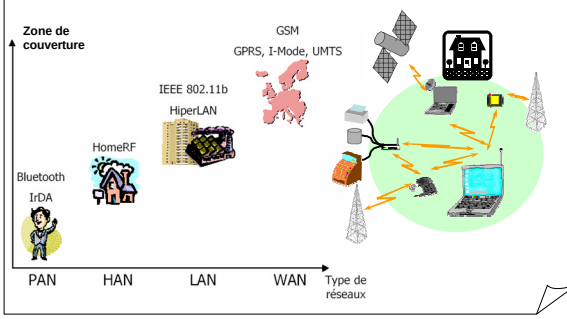
Notion de multi-trajets

- Exemple en intérieur



Types de réseaux sans fil

Couverture des réseaux sans fil



Couverture des réseaux sans fil

- **PAN** : Personal Area Network
  ~ quelques mètres autour de l'usager
  Ex : Bluetooth, IrDA
- **HAN** : Home Area Network
  ~ 10 mètres autour d'une station relais
  Ex : HomeRF
- **LAN** : Local Area Network (**WLAN** pour Wireless)
  ~ quelques dizaines de mètres, centaines de mètres
  Ex : DECT, IEEE 802.11
- **WAN** : Wide Area Network
  ~ quelques centaines / milliers de km
  Ex : GSM, GPRS, UMTS, CDMA, Satellites

Modes de transmission

Caractéristiques	Unidirectionnelle (Point à point)	Omnidirectionnelle
Portée	Importante (qq kms)	Faible
Vitesse	Elevée	Faible
Interférences	Rares	Fréquentes
Confidentialité	Bonne	Mauvaise Diffusion des transmissions
Applications	Interconnexion de 2 bâtiments sans passer par un opérateur (privée)	Gestion d'un parc de portables
Technologies Utilisées	Laser Infrarouge Micro-ondes Satellite Radio	Radio Infrarouge Micro-ondes

Principes fondamentaux

Principes fondamentaux

- Spécifiques au sans fil :
  - mobile, antenne, point d'accès, pont réseau, borne d'extension…
  - organisation cellulaire
  - mécanisme de handover

Mobile

- D'une unité logique
  - PC, PDA, Téléphone, …

- D'un émetteur / récepteur (*adaptateur*)
  - Interne (carte PCMCIA)
  - Externe

Antenne

Antennes directionnelles

Antennes
omni-directionnelles

Antenne

- Caractéristique pour tous les types d'antennes :
  - *Facteur de Mérite (G/T)*
    - Sensibilité d'un système de réception
    - Mesure globale du système de réception déterminé par la taille de l'antenne (G) utilisée et par la qualité (T) (niveau de bruit) du récepteur.
  - *Puissance Isotrope Rayonnée Équivalente (PIRE)*
    - puissance rayonnée dans une direction donnée ou dans la zone couverte.

Point d'accès

- Liaison réseau filaire - réseau sans fil
- Gère le trafic des mobiles d'une cellule
  en réception et en transmission de données
- Type de matériel : Station (dédiée de préférence) avec :
  - carte réseau traditionnelle pour le réseau filaire
  - carte émission / réception radio
  - couche logicielle adéquate

Borne d'extension

- Mélange Point d'accès (gère une cellule) + pont radio
- **Pas de connexion au réseau filaire (? point d'accès)**
- Agrandit la zone de couverture sans ajout de câble
- Gère le trafic de sa cellule comme les points d'accès
- Possibilité d'en utiliser plusieurs pour atteindre les mobiles les + éloignés.

Pont radio

- Lien entre 2 réseaux câblés
  de 100 m jusqu'à quelques kms
- Se connecte à un réseau et non à une station
- Ne gère pas de cellule de communication

Organisation cellulaire

- **Cellule de communication** =
  BSS : Basic Set Service

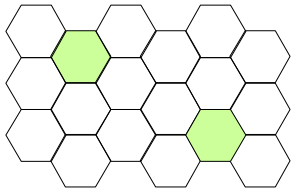
de taille variable :

- liée à l'environnement
- liée à la puissance du mobile, car le point d'accès (fixe) dispose à priori d'une source d'énergie suffisante

- **ESS** : Extended Set Service :
  plusieurs BSS <=> plusieurs AP (Access Point)

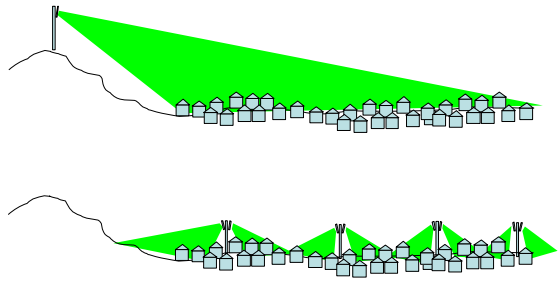
Organisation cellulaire

- Réutilisation de la même fréquence sur des zones géographiques différentes



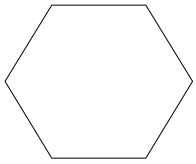
- Avantage : augmentation de la capacité
- Inconvénient : augmentation des interférences

Implantation des antennes

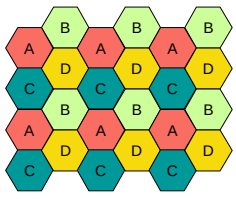


Exemple : couverture d'une zone

1 cellule



Organisation
en 6 clusters de 4 cellules



Ex: Bande passante de 100 MHz
200 KHz nécessaire par canal

100MHz pour la cellule
100M / 200K = **500 canaux**

100MHz / 4 cellules = 25 MHz par cellule
25M / 200K = 125 canaux par cellule
125 canaux *24 cellules = **3000 canaux**

Gain = nombre de clusters

Organisation cellulaire

- **Nombre d'utilisateurs** :

$$n = \frac{W}{B} x \frac{m}{N}$$

avec :

- W = largeur de la bande passante
- B = bande passante nécessaire par utilisateur
- N = facteur de réutilisation spectrale
  = nombre de cellules par cluster
- m = nombre total de cellules

Notion de qualité de service, prise en compte de la complexité, taille des terminaux, etc.

Organisation cellulaire

- **Plusieurs types de cellules** :
  - Femtocellules (qq mètres)
  - Picocellules (qq dizaines de mètres)
  - Microcellules (zone urbaine, antennes basses)
  - Macrocellules (zone urbaine, antennes hautes)
  - Megacellules Satellites (centaines de kms)
- Raisons : taille de la zone à couvrir, nombre d'utilisateurs, bâtiments, etc.

Organisation cellulaire

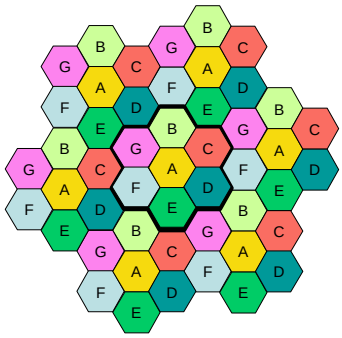
- Facteur de réutilisation

$$\frac{D}{R} = \sqrt{3N}$$

avec :

  - D = distance entre cellules
  - R = rayon de la cellule
  - N = taille du cluster

Exemple en zone urbaine, N=7



Organisation cellulaire

- Rapport signal sur interférences

$$SIR = \frac{P_{utile}}{\sum_i P_{interférence,i}}$$

- Pour deux stations de bases BS_1 et BS_2, avec un terminal à une distance d_1 et d_2 des BS émettant avec une puissance P_e

$$SIR = \frac{KP_e d_1^{-\alpha}}{KP_e d_2^{-\alpha}} = \frac{d_2^{\alpha}}{d_1^{\alpha}}$$

- Fréquences / cellules = Maximiser SIR

Organisation cellulaire

- Rapport signal sur interférences

$$SIR = \frac{d_0^{-\alpha}}{\sum_i d_i^{-\alpha}}$$

$$SIR \approx \frac{R^{-4}}{6D_L^{-4}} = \frac{1}{6}\left(\frac{D_L}{R}\right)^4 = \frac{3}{2}N^2$$

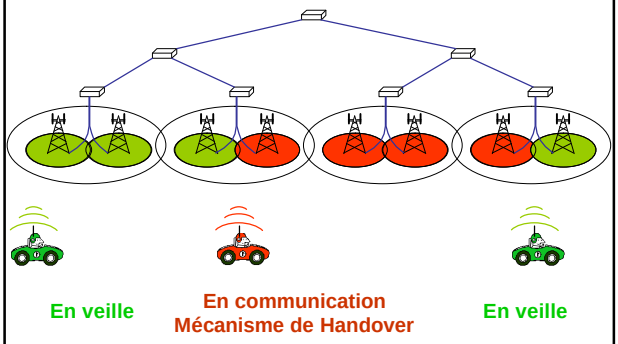
- en dB, SIR=-7,78+40 log(D_L/R)=1,76+20 log N

N	3	4	7	12	13	19
SIR en dB	11,3	13,8	18,6	23,3	24,0	27,34

Mécanisme de "Handover"

- Procédé issu du téléphone cellulaire GSM
- Permet au mobile de continuer un transfert commencé dans une cellule, dans une autre
  - Intercellulaire : passage d'une cellule à une autre (AP<->AP)
    - Si le signal est trop faible (en général)
    - Si un point d'accès sature (partage de trafic)
  - Intracellulaire :
    Changement de canal (si signal fort) avec qualité faible
  - Inter-réseau
    Très important pour les systèmes 3G
- On parle de *Handoff* dans les systèmes US

Mécanisme de "Handover"



Mécanisme de "Handover"

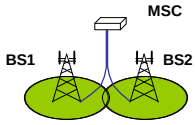
- Objectif :
  - assurer la continuité des communications tout en assurant une certaine qualité de service.
- Raisons :
  - optimiser l'utilisation des ressources
  - équilibrer le trafic entre cellules

➢ influe sur les aspects couches basses (physique et liaison)
➢ influe sur les aspects réseau (commutation de liens)

Mécanisme de "Handover"

- Exemple GSM
  - la qualité du lien est mesuré périodiquement
  - en cas de problème, la BS envoie une alarme vers le MSC
  - le MSC cherche une nouvelle cellule ou un nouveau canal
  - le MSC déclenche ensuite le handover si c'est possible (l'ancien canal est alors libéré), sinon la communication continue

MSC : Mobile Switching Center/Controller
BS : Base Station



Mécanisme de "Handover"

- le handover est tenté de plus en plus souvent :
  - réduction de la taille des cellules dans les systèmes 2G (numériques) (de plus en plus pour le milieu urbain = forte densité de population)
  - optimisation du trafic
- Contraintes :
  - obtenir des mesures précises de qualité
  - faire le bon choix pour le changement de cellule
  - réaliser rapidement le handover

Mécanisme de "Handover" : 3 phases

1. Mesures de qualité et de supervision du lien actif
   - puissance du signal reçu (RSSI : Received Signal Level Indicator).
   - le taux d'erreur binaire (BER : Bit Error Rate).
   - ratio C/I (Carrier/Interference)
   - distance entre le mobile et la station de base.

   Ex: GSM entre 3 et 10 mesures toutes les 0,5s

Mécanisme de "Handover"

2. Choix de la cellule cible

le mobile gère une liste de candidates (5 maxi en GSM) si il reçoit un signal suffisant pour le canal pilote

- puissance relative des signaux ($P_2 > P_1$)
- puissance relative des signaux avec seuil ($P_1 < \text{seuil}$ et $P_2 > P_1$)
- puissance relative des signaux avec hystérésis ($P_2 > P_1 + \text{seuil}$)
- puissance relative des signaux avec seuil et hystérésis ($P_1 < \text{seuil}_1$ et $P_2 > P_1 + \text{seuil}_2$)

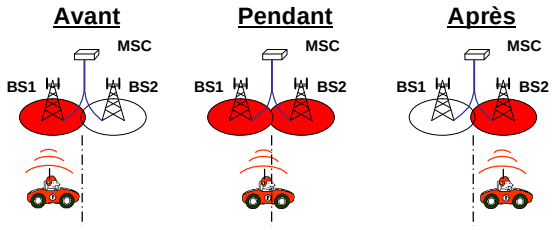
Mécanisme de "Handover"

3. Exécution du Handover
   – un nouveau canal est attribué
   – la connexion est transférée
   – l'ancien canal est libéré

- Différents types de Handover :
  – handover doux (soft-handover)
  – handover dur (hard-handover)
  – handover souple (smooth-handover)
  – …

Mécanisme de "Handover"

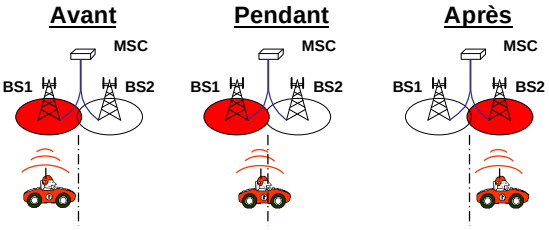
- Handover doux (soft-handover)



- Plus de consommation de ressources
+ Meilleur confort lors de passage d'une cellule à l'autre

Mécanisme de "Handover"

- Handover dur (hard-handover)



- Coupure de communication
  la + réduite possible en établissant le lien à l'avance
+ Pas de sur-consommation des ressources

Mécanisme de "Handover"

- **Handover souple** (smooth-handover)
  Pour les réseaux TCP/IP, le transport se fait par paquets indépendants : plus le nombre de paquets perdus est réduit, plus le handover est "souple"

- **Handover analogique**
  Aux États-unis, les systèmes de 1ère génération cohabitent avec les systèmes numériques :
  ➢ si les 2 systèmes et le terminal le permettent handover analogique pour assurer la continuité de la communication

Mécanisme de "Sélection / Re-sélection"

- Pour un mobile **en veille**, on parle de **sélection** de la station de base.
- Un mobile :
  – écoute les message diffusés par les BS à tous les mobiles
  – est prêt à se connecter au réseau en cas d'appel
  – signale sa position régulièrement
- La mise sous tension d'un mobile implique une sélection de BS.
- Le déplacement induit une **re-sélection** régulière.
- La gestion de la localisation = roaming
- Recherche de mobile = paging dans la dernière cellule ou dans tout le réseau (inondation)

Accès au réseau

- Le nombre d'utilisateurs est très supérieur au nombre de canaux disponibles
- Protocoles de réservation = problématique particulière
  – avec un contrôle centralisé → non
  – avec un contrôle distribué → non
  – à accès aléatoire (type CSMA)
  – autre…

Accès au réseau

- **CSMA** (Carrier Sense Multiple Access) a pour origine un système de communications par radio entre des machines sur les îles Hawaï (ALOHA - années 1970)
  Principe **ALOHA** : une station qui veut émettre… émet, si aucun accusé de réception, attente aléatoire et ré-émission.
- ➢ Très faible performance pour un fort trafic.
- Xerox, Intel & DEC : standard de fait pour un réseau Ethernet à 10 Mbit/s.
- ➢ Norme IEEE 802.3 - CSMA -CD

Accès au réseau

- **CSMA-CD** with Collision Detection
  dit CSMA 1-persistant
  - écoute du canal avant émission → réduction des collisions
    - si canal occupé, attente en écoutant
    - dès que le canal se libère émission
  - en cas de collision, attente aléatoire
  - performances supérieures

Accès au réseau

- **CSMA** non-persistant
  - si canal occupé, attente d'une durée aléatoire
  - à faible charge, beaucoup de bande passante gaspillée
- **CSMA** p-persistant
  - slot = temps maximal de propagation
  - si canal libre, émission avec probabilité *p*
    et attente du prochain slot avec probabilité *1-p*
  - si canal occupé, attente du prochain slot
  - ➢efficacité liée à l'optimisation de *p*

GSM

Historique GSM

- 1979 - Accord : 900 MHz pour le mobile
- 1982, Conférence Européenne des Postes et Télécommunications
  - 2 sous-bandes de 25 MHz
  - 890-915 MHz Mobile -> Réseau
  - 935-960 MHz Réseau -> Mobile
- GSM = Groupe Spécial Mobile - 13 pays Européens
  France / Allemagne (tout numérique)
- 1987, transmission numérique avec multiplexage temporel à bande moyenne
- En France : France Télécom et SFR / Alcatel et Matra
- Débuts en 1991, ouverture commerciale en 1992

Norme GSM

- ETSI = European Telecommunications Standards Institute <=> ANSI
- Norme adoptée en dehors de l'Europe
  - Concurrence : norme US et norme Japon

Norme GSM : Comités techniques

- SMG 1 - définition des services
- SGM 2 - interface radio
- SGM 3 - réseau fixe
- SGM 4 - services de données
- SGM 5 - Universal Mobile Telecommunication System
- SGM 6 - administration des réseaux
- SGM 7 et 8 - tests pour la station mobile et sous-système radio
- SGM 9 - carte SIM

GSM

- **Réussite** : spécifications complètes!!!
  - architecture
  - services
  - interface radio
  - …
  - GSM 900 et DCS 1800

Réseau GSM

- Architecture cellulaire : limite la puissance d'émission des mobiles = allonge l'autonomie
- Ondes radio :
  - Mobile vers BS (station de base)
  - BS vers Mobile
- 2 mobiles dans une même cellule ne communiquent pas directement

Cellule GSM

- Typiquement une cellule hexagonale avec une station de base BS (ou BTS) = tour avec antennes Base Transmitter Station
- GSM 900 MHz, distance mobile-BS = 35 kms max macro-cellule
- DCS 1800 MHz, distance mobile-BS = 2 kms max mini-cellule
  - puissance plus faible
  - atténuation plus importante des hautes fréquences avec la distance

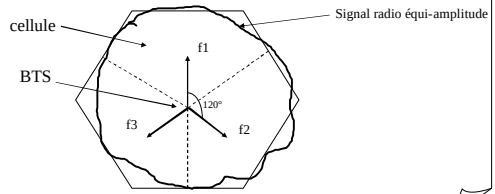
Cellule GSM

- station principale = antenne sur mât, pylône
- "sous-station" en ville principalement (rues encaissées, tunnels, bâtiments, …)
  = antennes peu élevées, boucles radio enterrées ou dans les murs, câbles rayonnants avec des fentes dans l'enveloppe extérieure
  - utilisation de répéteurs

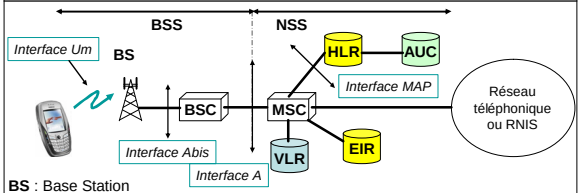
Cellule GSM

Les émetteurs sont généralement constitués de 3 antennes réparties à 120°. La répartition du signal radio équi-amplitude forme en première approximation un hexagone.

(un émetteur muni d'une seule antenne omni-directionnelle a un diagramme sensiblement équivalent).



Structure du réseau



BS : Base Station
BSC : BS Controller (contrôle entre 20 et 30 BS)
BSS : BS System = interface radio (équipement physique de la cellule)

MSC :Mobile services Switching Center = commutateurs mobiles
VLR : Visitor Location Register = base d'enregistrement des visiteurs (dynamique)
HLR : Home Location Register = BdD de localisation, caractérisation des abonnés
AUC : Authentification Center = centre d'authentification des abonnés
EIR : Equipement Identity Register = base de données des terminaux

BS : Station de base

- Émetteur / récepteur (TRX)
- Modulation / démodulation, égalisation, codage, correction d'erreur
- Mesures radio (transmises au BSC)
- Un TRX = 1 porteuse = 7 communications
  - Rural BTS=1 TRX, Urbain BTS=2-4 TRX
- **BTS Standard** (2,5-32 Watt)
  - Locaux techniques
  - Antennes + câble + coupleur + 1-4 TRX
- **Micro-BTS** (0.01-0.08 Watt)
  - Zone urbaine dense
  - Équipement intégré
  - Coût faible

BSC : Contrôleur de stations de base

- Gère les ressources radio
  - allocation de fréquences pour les communications
  - mesures des BTS, contrôle de puissance des mobiles et BTS
  - décision et exécution des handovers
- Rôle de commutateur

Ex: Plusieurs dizaines de BSC à Paris

HLR

Base de données de gestion abonnés

- Mémorise les caractéristiques d'un abonné
  - **IMEI** - *International Identification Equipment Identity* : numéro unique dans le mobile lors de sa fabrication
  - Numéro d'abonné
    IMSI - *International Mobile Subscriber Identity* se trouve dans la carte
    SIM - *Subscriber Identity Module*
  - Profil d'abonnement
- Mémorise le **VLR** où l'abonné est connecté (même à l'étranger) pour permettre l'acheminement éventuel d'un appel entrant

MSC, VLR et EIR

- MSC : Commutateur de services mobiles
- Communication mobile vers autre MSC
- Handover si hors BSC
- Gère le VLR pour la mobilité des usagers (identité temporaire)
- Fonction de passerelle avec RTC

- VLR : stocke dynamiquement les informations des abonnés liées à leur mobilité
- EIR : Equipement Identity Register = identité des terminaux, contrôle d'homologation, déclaration de vol, etc.

MSC

OMC

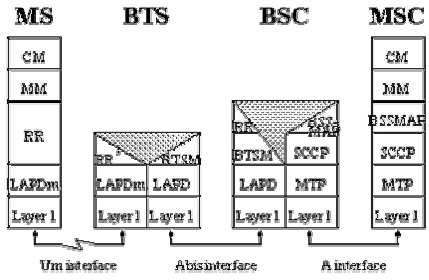
Operation and Maintenance Center

- Poste de surveillance de l'ensemble du réseau. Une partie de l'OMC surveille la partie BSS (BTS et BSC), c'est OMC-Radio (OMC-R), l'autre partie surveille la partie NSS, c'est l'OMC-S (OMC-Commutation (Switch)).
- Chacun d'eux remonte l'ensemble des alarmes majeures ou mineures issues du réseau. L'OMC est l'outil de maintenance (curative). Il permet des interventions à distance (logicielles).

BSS – sous-système radio

- Couche 1 physique
- Couche 2 liaison de données
  - fiabilisation de la transmission (protocole)
- Couche 3 réseau
  - gestion des circuits commutés
  - Radio Ressource (RR)
    - gestion des canaux logiques
    - surveillance des balises
  - Mobility Management (MM)
    - localisation/authentification/allocation identité temporaire
  - Connection Management (CM)
    - Call Control, Short Message Service, Supplementary Services

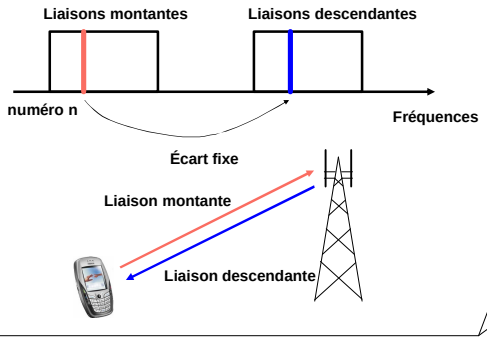
Interfaces et protocoles



Fréquences utilisées

- Bande **EGSM** (GSM étendue) :
  - largeur 35 MHz
  - de 880 à 915 MHz Mobile → Base
  - de 925 à 960 MHz Base → Mobile
  - écart de 45 MHz
  - 174 canaux de 200KHz
- Bande **DCS** :
  - largeur 75 MHz
  - de 1710 à 1785 MHz Mobile → Base
  - de 1805 à 1880 MHz Base → Mobile
  - écart de 95 MHz
  - 374 canaux de 200KHz

Exemple



Fréquences utilisées

- Atténuation en $1/f^2$
  Les hautes fréquences se propagent moins loin pour une même puissance
- DCS plutôt réservé aux zones urbaines à forte densité de trafic (nécessite plus de stations de base)

Fréquences utilisées

- Numéro n codé sur 10 bits

Voie descendante :

- pour 1 = n = 124 f=935+(0,2xn) GSM
- pour 975 = n = 1024 f=935+(0,2x(n-1024)) EGSM
- pour 512 = n = 885 f=1805,2+(n-512) DCS

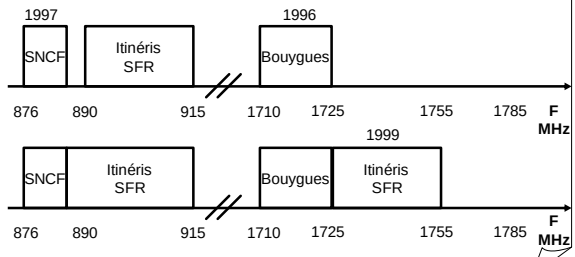
Voie montante :

- calculée avec l'écart duplex fixe

- Réseaux mixtes possibles : terminaux bi-bandes nécessaires

Fréquences utilisées

- Attribution des fréquences : évolue dans le temps
- Bande montante :



Voie balise et voie trafic

- Chaque station de base émet en permanence des informations sur sa voie balise (BCH = Broadcast Channel)
- Un mobile en veille échange avec sa BS des signaux de contrôle (émission en slot 0 à f, réception en slot 0 à f+écart)
- Le niveau de la voie balise (BCH) est connu pour :
  - à la mise en route, chercher le niveau le + élevé pour se connecter à une BS
  - émettre des infos opérateurs et fréquences des cellules voisines
  - messages affichés sur l'écran du mobile

Voie balise et voie trafic

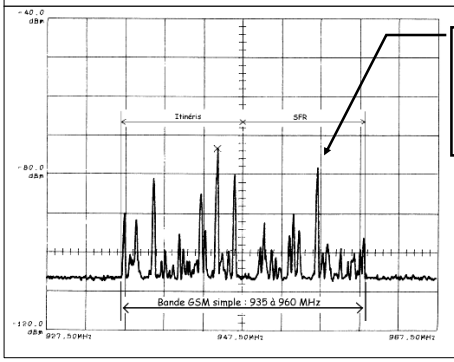
Mobile en veille :

- Un récepteur écoute les BCH des cellules voisines toutes les 5s si le signal reçu est faible, toutes les 15s si le signal est fort
- La liaison montante est utilisée pour des demandes de connexion (RACH)

Mobile en communication :

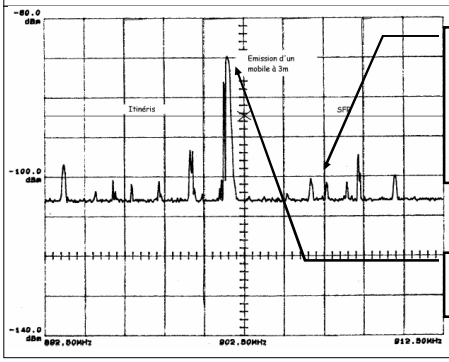
- Échange des signaux de parole et de contrôle sur la voie TCH (émission en slot i à f, réception en slot i à f+écart)
- Écoute des voies balises pour un éventuel changement de cellule

Spectre de la bande GSM descendante



Voie balise de la cellule la plus forte pour un opérateur

Spectre de la bande GSM montante

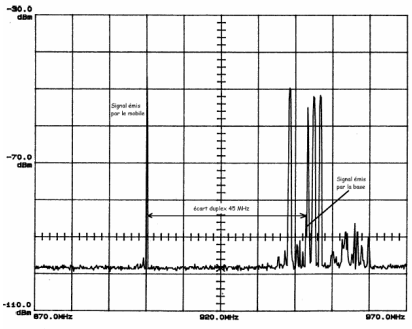


Pics : correspondent à l'allumage des mobiles

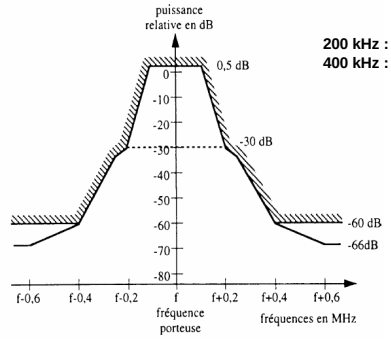
Superposition de 2h d'enregistrement

Communication proche de l'enregistreur

Spectres de la bande montante et descendante pendant une conversation

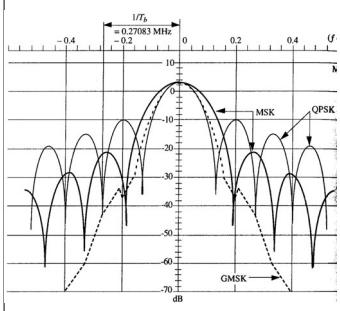


Encombrement spectral d'un signal GSM



200 kHz : -30 dB
400 kHz : -60 dB

Modulation GMSK



Gaussian Minimum Shift Keying ≈ combinaison de modulation de phase et de fréquence.

Largeur de bande: 200 kHz

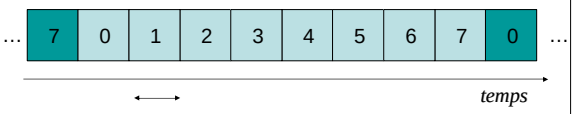
Débit binaire: 270.833 kbps

1 bit = 3.7 µs

Multiplexage temporel : TDMA

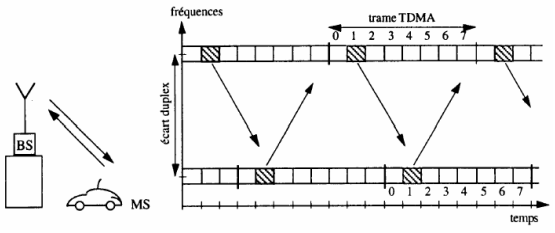
8 Time Slots par canal

Durée d'une trame TDMA = 4.62 ms



7500 x 1/13 MHz = **577 ms**
(7500 périodes de Quartz de mobile)
156.25 bit
270 kbps

Multiplexage temporel : TDMA



Réception puis émission 3 time-slots après (1,7ms) pour le mobile :
- évite la simultanéité des traitements
- la synchronisation elle-même est décalée

Codage de la parole

- Le codage consiste à comprimer de façon efficace les données de telle sorte à minimiser le débit requis et donc rentabiliser les ressources mises à disposition.
- Compte tenu du spectre de la voix (300 - 3400 Hz), la numérisation du signal perçu par le microphone nécessiterait un débit de 64 kbit/s.

  => C'est un trop haut débit, donc on utilise un codage spécifique.

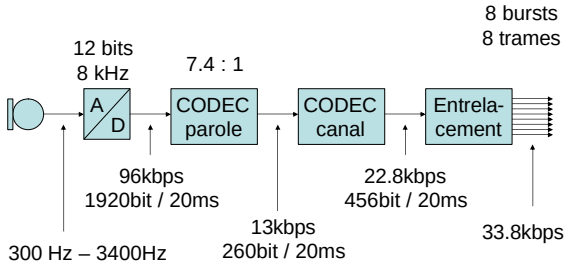
Codage de la parole

- Le codeur utilisé dans la norme GSM est un codeur donnant un débit de 13 kbit/s.
  - Principe :

    La parole est analysée par tranche de 20 ms et codée sur 260 bits (13 kbit/s).

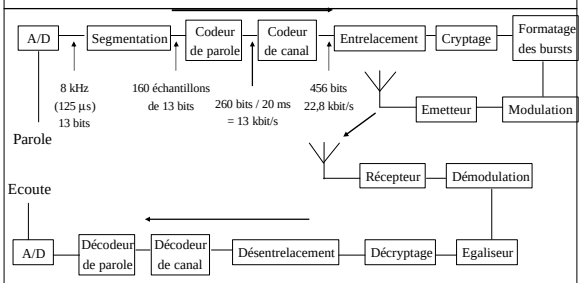
- Le codage de canal ajoute de la redondance à ce signal afin de lui donner de la robustesse face au canal de propagation radio. On aboutit à un codage sur 456 bits (22,8 kbit/s).

Codage de la parole



A/D : convertisseur Analogique -> Digital

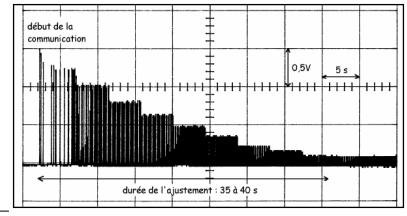
Codage de la parole



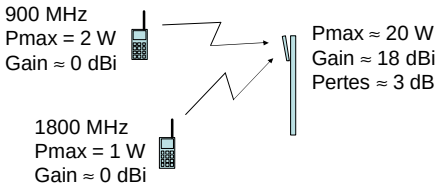
L'entrelacement : Des paquets d'erreurs ont lieu sur un canal radiomobile. Ces paquets sont générés par des évanouissements qui peuvent être de même durée que le burst, il convient de répartir les données sur plusieurs trames consécutives.

Contrôle de puissance d'émission

- La station de base contrôle de nombreux paramètres du mobile dont la puissance d'émission :
  - minimisation de $P_{émis}$ tout en conservant la QoS
    - diminution des interférences
    - augmentation de l'autonomie



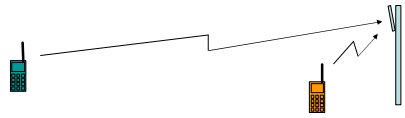
Puissance



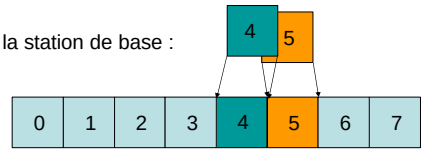
La puissance varie par pas de 2 dB jusqu'à une réduction maximale de 20 dB (99%).

Gestion des retards

Retard maxi = 2 x 35 km = 233 µs (300 000 km/s)

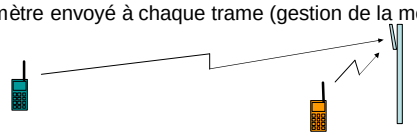


Au niveau de la station de base :

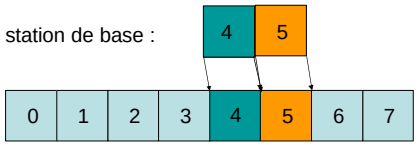


Gestion des retards =Timing Advance
(paramètre TA)

Max 2 x 35 km = 233 µs => 64 valeurs (6 bits)
paramètre envoyé à chaque trame (gestion de la mobilité)



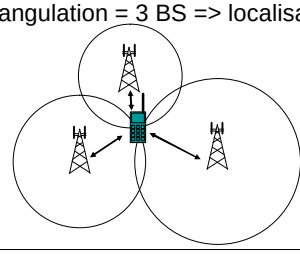
Au niveau de la station de base :



Résolution: 1 bit = 3.7 µs = 2 x 550 m

Positionnement, localisation

- La connaissance de ce paramètre pour une station de base permet de connaître la distance au mobile
- Avec triangulation = 3 BS => localisation

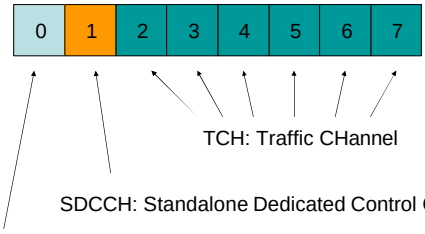


Changement de cellule

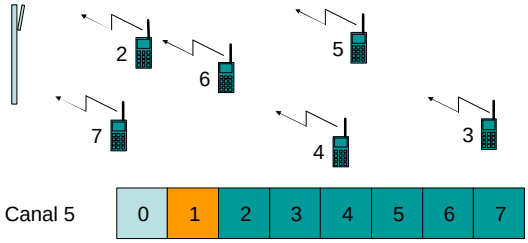
- Lors d'une conversation, le mobile écoute les BCH des cellules voisines. L'écoute se fait entre l'émission et la réception du *burst* suivant : mesure de niveau (peu de temps)
- Pour décoder les informations, le mobile s'arrête d'émettre et de recevoir toutes les 26 trames (slot *idle*): le mobile écoute et décode la voie balise de l'une des cellules voisines. Quant à la station de base, elle émet les informations toutes les 51 trames.
  51 et 26 étant premiers entre eux, toutes les voies balises seront décodées:
  Trames décodées : 0,26,1,27,2,28…

26+26-51

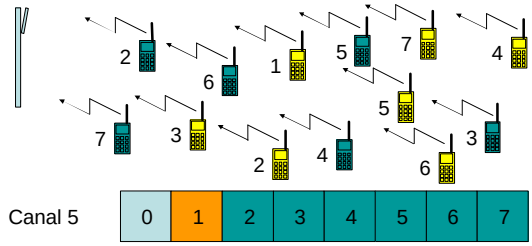
Canaux logiques



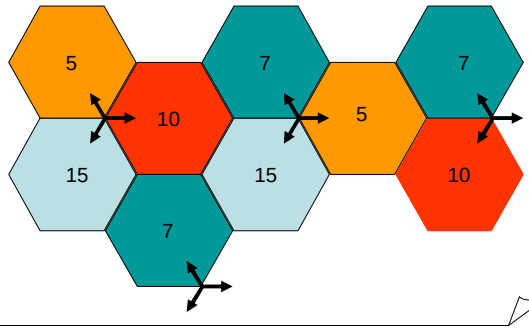
Trafic / Capacité (1/2)



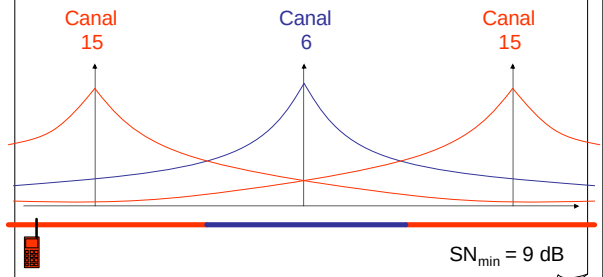
Trafic / Capacité (2/2)



Réutilisation des fréquences



Réutilisation et interférences



Mobile en fonctionnement

A la **mise sous tension** se passent les opérations suivantes :

- l'utilisateur valide sa carte SIM en tapant au clavier son numéro de code PIN (Personal Identity Number)
- le récepteur du (GSM scrute les canaux de la bande (GSM et mesure le niveau reçu sur chaque canal
- le mobile repère le canal BCCH parmi les signaux les plus forts
- le mobile récupère les informations concernant le FCCH. Ce signal lui permet de se caler précisément sur les canaux GSM
- le mobile récupère le signal de synchronisation de la trame TDMA diffusé sur le BCCH et synchronise sa trame
- le mobile lit sur le BCCH les infos concernant la cellule et le réseau et transmet à la BTS l'identification de l'appelant pour la mise à jour de la localisation

Le mobile a alors achevé la phase de mise en route et se met en mode veille, mode dans lequel il effectue un certain nombre d'opérations de routine :

- lecture du PCH (Paging channel) qui indique un appel éventuel
- lecture des canaux de signalisation des cellules voisines
- mesure du niveau des BCH des cellules voisines pour la mise en route éventuelle d'une procédure de handover

Mobile en fonctionnement

A la **réception** d'un appel :

- l'abonné filaire compose le n° de l'abonné mobile: 06 XX XX XX XX
- l'appel est aiguillé sur le MSC le plus proche qui recherche l'IMSI dans le HLR et la localisation du mobile dans le VLR
- le MSC le plus proche du mobile (Visited MSC : fait diffuser dans la zone de localisation, couvrant plusieurs cellules, un message à l'attention du mobile demandé par le PCH)
- le mobile concerné émet des données sur RACH avec un Timing Advance fixé à O et un niveau de puissance fixé par le réseau (ces paramètres seront ajustés ultérieurement)
- le réseau autorise l'accès par le AGCH et affecte au mobile une fréquence et un time-slot
- l'appelé est identifié grâce à la carte SIM
- le mobile reçoit la commande de sonnerie
- décrochage de l'abonné et établissement de la communication

Mobile en fonctionnement

Lors de **l'émission** d'un appel

- l'abonné mobile compose le numéro du correspondant du réseau téléphonique commuté
- la demande arrive à la BTS de sa cellule
- elle traverse le BSC pour aboutir dans le commutateur du réseau MSC
- l'appelant est identifié et son droit d'usage vérifié
- l'appel est transmis vers le réseau public
- le BSC demande l'allocation d'un canal pour la future communication
- décrochage du correspondant et établissement de la communication

Localisation - itinérance

- Lors d'un appel entrant, pour contacter un mobile :
  - on envoie un message de recherche (paging)
    - dans la dernière cellule auquel le mobile s'est enregistré
    - dans tout le réseau (inondation)
  - recherche avec les bases de données
    - centralisées
    - décentralisées
    - hybrides

GSM : canaux logiques

- Catégories
  - Broadcast Channel (groupe BCH)
    - Voie descendante, voie balise
  - Common Control Channel (groupe CCCH)
    - Voie descendante et montante
  - Dedicated Control Channel (groupe DCCH)
    - Voie descendante et montante
  - Traffic Channel (groupe TCH)
    - Voie descendante et montante

GSM : canaux logiques

- Groupe BCH
  - **Frequency Correction Channel (FCCH)**
    - Calage sur la fréquence porteuse
      - Signal sinusoïdal parfait
  - **Synchronisation Channel (SCH)**
    - Synchronisation et identification
      - Burst d'apprentissage identique dans tout le réseau
      - Code BISC (couplé avec la fréquence, on identifie la cellule)
  - **Broadcast Control Channel (BCCH)**
    - Information sur le système
      - Numéro de ZaC, paramètre de sélection des cellules, paramètres pour l'accès aléatoire, description des canaux logiques, description des cellules voisines...

GSM : canaux logiques

- Groupe CCCH
  - Paging Channel (PCH)
    - Paging pour SMS et demande d'appel (réponse du mobile sur le RACH)
  - Random Access Channel (RACH)
    - Montant, accès aléatoire (demande des mobiles)
  - Access Grant Channel (AGCH)
    - Message d'allocation d'un canal de signalisation (SDCCH) et Timing Advance
  - Cell Broadcast Channel (CBCH)
    - Diffusion d'informations « applications » (météo, routes)

GSM : canaux logiques

- Groupe DCCH
  - **Stand-Alone Dedicated Control Channel (SDCCH)**
    - Pour le Setup et pour mise à jour de localisation
  - **Slow Associated Control Channel (SACCH)**
    - Instrumentation d'un canal de trafic (TCH ou SDCCH)
      - Contrôle de puissance, contrôle qualité radio, rapatriement des mesures
  - **Fast Associated Control Channel (FACCH)**
    - Extension de la capacité du SACCH par vol de slot aux canaux qu'il instrumente
    - Utilisation en Handover uniquement

GPRS

GPRS

- **GPRS** (General Packet Radio Service) : transfert de données par paquet sur GSM (modulation GMSK) vers Internet et réseaux X25 : jusqu'à 171 kbit/s (suivant le codage de canal CS-1 à CS-4)

Codage de canal	Débit Utile	Protection
CS-1	9,05 kbit/s	++
CS-2	13,4 kbit/s	+
CS-3	15,6 kbit/s	-
CS-4	21,4 kbit/s	-- (aucune protection)

Facturé au débit - MMS

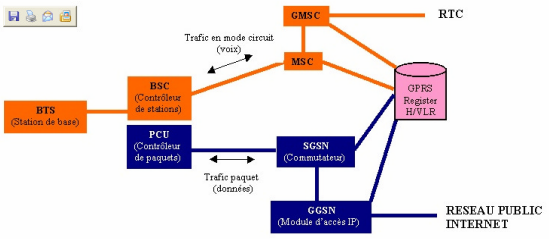
GPRS

- Échange de données en mode paquets :
  - découper l'information et transmettre les données par paquet lorsque les canaux ne sont pas utilisés pour la phonie
  - optimise les ressources radio par gestion de priorité, mise en attente et affectation de ressources radio uniquement en cas de transfert
- Un canal radio peut être utilisé par plusieurs utilisateurs. Les Time Slots sont partagés => moins de blocage.
- Un utilisateur peut utiliser plusieurs canaux radio. Les Time Slots sont agrégés => débits plus importants.

GPRS

- Sur les timeslots d'un TRX, certains sont alloués au GPRS, mais la voix a toujours la priorité
- Utilise la capacité libre
- On peut utiliser jusqu'à 8 Time Slots (8 x 21.4 kbit/s + header = 171 kbit/s pour CS-4).
- La transmission peut se faire indépendamment en UpLink et en DownLink mais pas forcément en simultané (suivant le type de mobile)
- Généralement, on alloue plus de Time Slots en DownLink qu'en UpLink.

GPRS : structure du réseau



GPRS : structure du réseau

- L'implantation du GPRS peut être effectuée sur un réseau GSM existant. Les BS ne subissent aucune modification si ce n'est l'adjonction d'un logiciel spécifique, qui peut être installé par téléchargement.
- Plus en amont, le contrôleur de stations de base doit être doublé par un contrôleur de paquets (PCU pour Paquets Controler Unit).
- Vient ensuite, la chaîne destinée aux données par paquets, constituée du commutateur (SGSN) ou Switch spécifique GPRS, équivalent du Mobile Switch Controler (MSC), contrôleur qui a pour fonction de vérifier l'enregistrement des abonnés, de les authentifier et d'autoriser les communications, et du module d'accès (GGSN) au monde IP (Internet ou Intranet).
- Le GGSN et le SGSN sont expliqués dans la partie suivante.
- Sans licence GSM, il n'est pas possible d'installer un réseau GPRS.

GPRS : structure du réseau

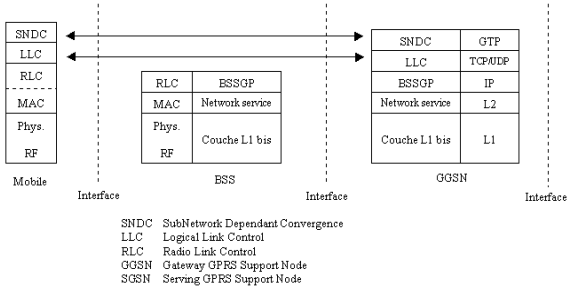
- GGSN : *Gateway GPRS Support Node* ou Routeur IP s'interfaçant avec les autres réseaux :
  - fonctionnalité d'interconnexion dans le centre de communication (MSC), qui permet de communiquer avec les autres réseaux de données par paquets extérieurs au réseau GSM.
  - masque au réseau de données les spécificités du GPRS. Il gère la taxation des abonnés du service, et doit supporter le protocole utilisé sur le réseau de données avec lequel il est interconnecté.
  - Les protocoles de données supportés en standard par un GGSN sont IPv6, CLNP et X25. SGSN : *Serving GPRS Support Node* ou Routeur IP gérant les terminaux pour une zone.

GPRS : structure du réseau

Le SGSN (Serving GPRS Support Node) :

- fonctionnalité du service dans le centre de commutation (MSC), qui permet de gérer les services offerts à l'utilisateur.
- interface logique entre l'abonné GSM et un réseau de données externe.
- missions principales :
  - gestion des abonnés mobiles actifs (mise à jour permanente des références d'un abonné et des services utilisés)
  - relais des paquets de données. Quand un paquet de données arrive d'un réseau PDN (Packet Data Network) externe au réseau GSM, le GGSN reçoit ce paquet et le transfert au SGSN qui le retransmet vers la station mobile. Pour les paquets sortants, c'est le SGSN qui les transmet vers le GGSN.

GPRS : couches logicielles



SNDC SubNetwork Dependant Convergence
LLC Logical Link Control
RLC Radio Link Control
GGSN Gateway GPRS Support Node
SGSN Serving GPRS Support Node

GPRS : couches logicielles

Dans le terminal mobile, nous trouvons de bas en haut les couches suivantes :

- La couche physique, qui se décompose en deux sous-couches fonctionnelles ;
  - La sous-couche RF, qui gère les fonctions radio du terminal. Elle émet les informations reçues de la couche physique. Elle décode les informations reçues de la station de base et les transfère pour interprétation vers la couche physique ;
  - La couche physique produit les trames, qui seront émises par la couche radio ; pour les trames reçues du réseau, elle détecte et corrige les erreurs de transmission ;
- La couche MAC (ou RLC pour Radio Link Control) pilote la liaison radio entre le terminal et la station de base, c'est-à-dire les mécanismes de retransmission en cas d'erreur, la fonction de contrôle d'accès aux ressources radio quand plusieurs terminaux sont en concurrence. Le RLC peut demander la retransmission d'un bloc de données ;
- La couche supérieure SNDC (SubNetwork Dependant Convergence) gère la mobilité, le cryptage et la compression de données.

GPRS : routage des paquets

- Le routage de chaque paquet est indépendant de celui qui le précède ou de celui qui le suit.
- Pendant la phase de connexion d'un terminal dans un réseau GSM, les échanges de signalisation sont nombreux, et pour faire face aux contraintes du mode paquet, les informations de routage obtenues pour acheminer le premier paquet vers un terminal GSM sont stockées dans le GGSN.
- Ainsi la route pour les paquets suivants est sélectionnée à partir du contexte stocké dans le GGSN (le Temporary Logical Link Identity ou TLLI).

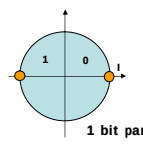
EDGE

EDGE

- **EDGE** (Enhanced Data rate for GSM Evolution) ou EGPRS
  - Le débit max du GPRS n'est valable que pour des C/I importants (utilisation du CS-4), ce qui n'est pas toujours le cas.
  - On va donc changer de modulation GMSK => 8-PSK. La vitesse de modulation est la même que pour le GMSK mais permet un débit instantané 3 fois plus élevé, chaque état de modulation transmettant l'information relative à 3 bits.
  - Débits du EDGE
    - 6 débits sont normalisés de PCS-1 à PCS-6 variant de 22,8 kbit/s à 69,2 kbit/s par Time Slot.
    - Le débit max instantané sera donc de 553 kbit/s (moy # 300 kbit/s).

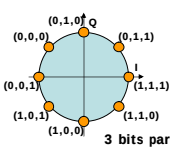
EDGE

- En cours de développements.
- Nécessite le remplacement des émetteurs-récepteurs et terminaux
- Compatible avec le reste des équipements



1 bit par symbole

Modulation GMSK



3 bits par symbole

Modulation EDGE

UMTS

UMTS

- (*Universal Mobile Telecommunication System*)
- Jusqu'en 1995 : définition des objectifs et contraintes des aspects essentiels de l'UMTS : cadre d'application, services, interfaces radio, plate-forme réseau, gestion, systèmes satellites, etc.
- Spécifications détaillées en 1998 : premiers produits sortent et disponibilité des services à partir de 2005.
- Le principe de l'UMTS est souvent résumé dans la formule *anyone*, *anywhere*, *anytime*, signifiant que chacun doit pouvoir joindre/être joint, n'importe où et n'importe quand. Le système doit permettre l'acheminement des communications indépendamment de la localisation de l'abonné, que celui-ci se trouve chez lui, au bureau, en avion, …

UMTS

- L'UMTS doit répondre aux besoins de toutes les populations d'usagers et en particulier il doit regrouper les fonctionnalités et avantages des systèmes existants :
- qualité de parole élevée et couverture étendue comme les systèmes cellulaires,
- appels de groupe, diffusion de messages, accès rapide et faibles coûts comme les systèmes de radiocommunications privés,
- terminaux de petite taille et couverture dense à l'instar des systèmes de radiomessagerie unilatérale,
- communications de débit élevé et d'excellente qualité comme pour les systèmes sans cordon,
- couverture mondiale des systèmes satellites,
- accès à des sites distants comme pour les réseaux de transmission de données.

UMTS

- Quelques caractéristiques importantes permettent ainsi d'identifier les systèmes de troisième génération :
- interface radio pouvant s'adapter aux différentes méthodes d'accès multiple (FDMA/TDMA/CDMA) en fonction des sites,
- terminaux capables de télécharger leur système d'exploitation en fonction du réseau et de l'évolution du système,
- architecture s'appuyant sur les principes du réseau intelligent,
- capacité d'interfonctionnement avec le réseau fixe de façon totalement transparente pour les usagers,
- portabilité des services de type RNIS.

UMTS

- L'UMTS sera donc un réseau structuré autour des trois concepts de réseaux suivants
- réseaux d'accès (*Access Networks*) assurant la transmission de base des informations (signalisation et trafic), la commutation locale pour l'accès au réseau fixe,
- réseaux fédérateurs (*Backbone Networks*) qui intègrent l'infrastructure de base du réseau fixe et les ressources radio (contrôle d'appel et gestion des connexions typiquement),
- réseaux de services (*Services Networks*) assurant le stockage et la gestion des données ainsi que le traitement des services offerts aux usagers.

UMTS – Anciennes prévisions

	2002	***2005***
Services	Multimédia 144 kbit/s - 2 Mb/s Création de services Portabilité du service Itinérance GSM/UMTS	Multimédia enrichi Itinérance avec d'autres réseaux FPLMTS
Terminaux	Adaptatifs téléchargeables Bi-mode/bi-bande GSM/UMTS	Capacités multimédia enrichies
Réseau d'accès	Nouveau BSS à 2 GHz Efficacité spectrale	Utilisation ATM élargie Nouvelle(s) bande(s)
Réseau de transport	Évolution de GSM Convergence mobile/fixe	Support de multimédia amélioré pour l'utilisation de l'ATM

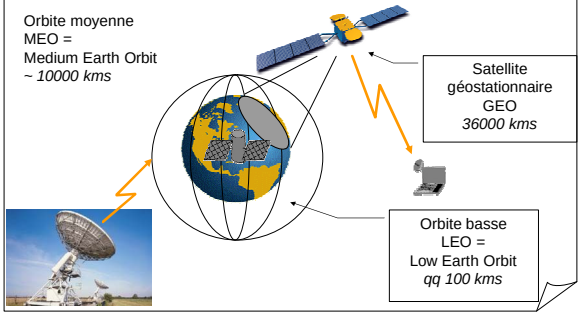
UMTS

- La 3ème génération de téléphonie mobile est l'UMTS (Universal Mobile Telecommunication System).
- Cette nouvelle norme repose sur les technologies W-CDMA (combinaison de CDMA et FDMA) et TD-CDMA (combinaison de TDMA, CDMA et FDMA).
- Le principe de transmission repose sur l'étalement de spectre et la modulation QPSK.
- Les fréquences utilisées sont 2 bandes appairées (1920-1980 MHz et 2110-2170 MHz) et 2 bandes non appairées (1900-1920 MHz et 2010-2025 MHz).
- Cette technologie va permettre la transmission de données en mode paquet (et en mode circuit) à des débits d'environ 2 Mbit/s.

Satellites

Satellites

- Différentes orbites : GEO, MEO, LEO



Satellite GEO

- Simple à mettre en œuvre
- Même vitesse angulaire que la terre (semble fixe)
- Couverture globale : 3 satellites seulement
- Nombre total limité
  (angle <2° => interférences entre satellites)
- Orbite ~ 36000 Kms
- Délai (A/R) : 250 ms (important)
- Applications : Diffusion, VSAT, liaison point à point
- Débit : jusqu'à 155 Mb/s
- Exemples : Astra, Hotbird …

Satellite MEO

- Orbite : 10000 Kms
- Délai (A/R) : 80 ms
- Applications : voix (mobiles), data bas débit
- Débit : 300b/s à 38.4 kb/s
- Exemples : Odyssey, Ellipso

Satellite LEO

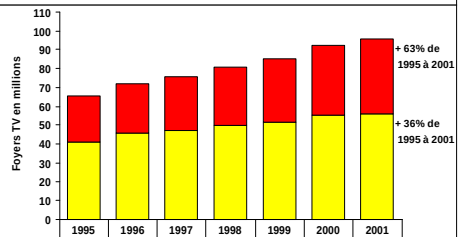
- Orbite : 640 à 1600 Kms
- Délai (A/R) : 6 à 21 ms (~ négligeable)
- Couverture globale : environ 40 à 900 satellites
- Applications : voix (mobiles), data haut & bas débit
- Débit : 2.4 kb/s à 155 Mb/s
- Exemples : Iridium, Globalstar, Télédesic ...

Satellites TV :

mode de réception ayant la croissance la plus dynamique

Source ASTRA

Satellite : croissance en Europe*

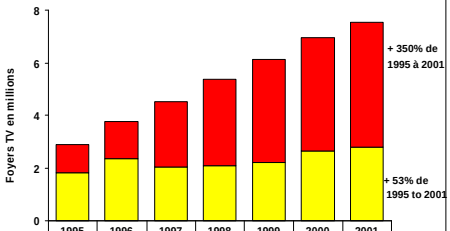


	1995	1996	1997	1998	1999	2000	2001
Total Réception directe & Câble	65,47	71,78	75,76	80,78	85,36	92,23	95,69
Réception directe	24,29	25,96	28,74	31,12	33,91	37,02	39,61
Câble	41,18	45,81	47,02	49,66	51,45	55,21	56,08

*Europe : 22 pays inclus

Source: Études de marché de la réception satellite en Europe

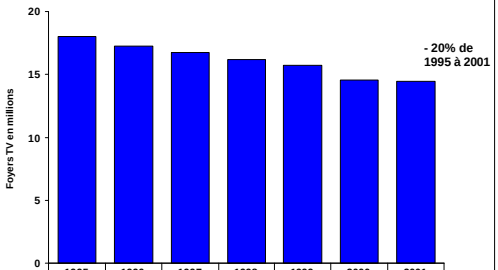
Satellite : croissance en France



	1995	1996	1997	1998	1999	2000	2001
Total Réception directe & Câble	2,89	3,76	4,52	5,36	6,11	6,96	7,54
Réception directe	1,05	1,40	2,47	3,26	3,92	4,30	4,74
Câble	1,83	2,36	2,05	2,10	2,19	2,66	2,80

Source: Études de marché de la réception satellite en France, Institut français de Démoscopie

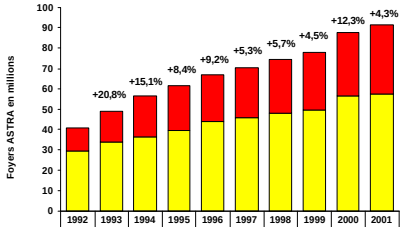
La réception hertzienne en France



	1995	1996	1997	1998	1999	2000	2001
Réception hertzienne	18,01	17,23	16,76	16,21	15,70	14,57	14,47

Source: Études de marché de la réception satellite en France, Institut français de Démoscopie

ASTRA : leader de la réception directe en Europe*

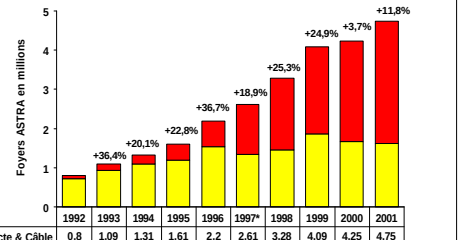


	1992	1993	1994	1995	1996	1997	1998	1999	2000	2001
Total Réception directe & Câble	40,72	49,18	56,58	61,33	66,97	70,52	74,54	77,93	87,51	91,32
Réception directe	11,22	15,43	19,99	21,73	22,97	24,78	26,51	28,25	30,94	33,67
Câble	29,50	33,75	36,59	39,60	44,00	45,74	48,03	49,68	56,57	57,65

*30 pays européens, dont 8 pays d'Europe de l'Est à partir de 2000

Source: Études de marché de la réception satellite en Europe

ASTRA : leader en France



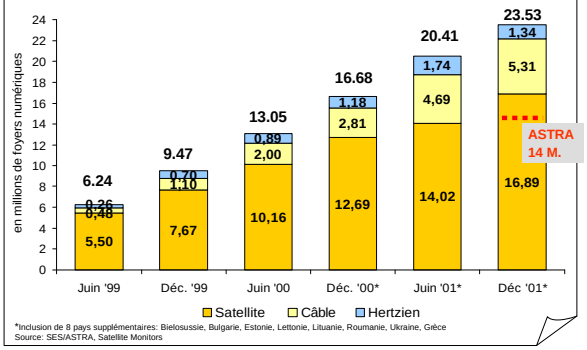
Au 31 déc.

	1992	1993	1994	1995	1996	1997*	1998	1999	2000	2001
Total Réception directe & Câble	0,8	1,09	1,31	1,61	2,2	2,61	3,28	4,09	4,25	4,75
Réception directe	0,09	0,16	0,22	0,42	0,66	1,28	1,83	2,23	2,58	3,12
Câble	0,71	0,93	1,09	1,19	1,54	1,33	1,45	1,86	1,67	1,63

*Modification de la méthodologie depuis fin 1997

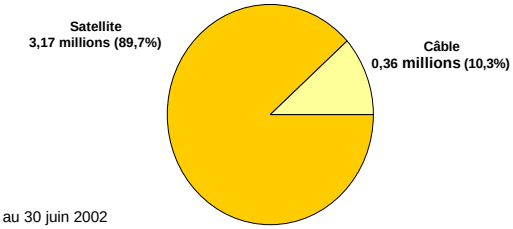
Source: Études de marché de la réception satellite en France, Institut français de Démoscopie

Réception numérique en Europe: satellite dans 7 foyers sur 10



*Inclusion de 8 pays supplémentaires: Bielosussie, Bulgarie, Estonie, Lettonie, Lituanie, Roumanie, Ukraine, Grèce
Source: SES/ASTRA, Satellite Monitors

Structure du marché numérique – France



au 30 juin 2002

Base: 3,53 millions de foyers numériques

Source: Études de marché de la réception satellite en France, Institut français de Démoscopie

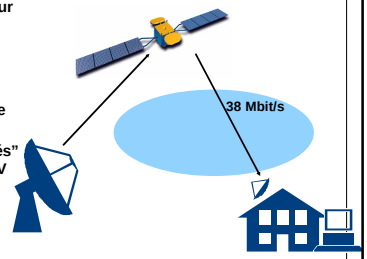
Consolidation: un marché en pleine évolution

- Marché des opérateurs satellitaires:
  - Excédent de capacité en orbite
  - Développement différé des services à bande large par satellite
  - Privatisation des opérateurs satellitaires organisés sous forme d'organisations intergouvernementales

Services à large bande par satellite

▲ **Distribution de services à voie unique avec voie de retour terrestre**

- ➢**Services**
  - ▪**A-DSL par satellite pour particuliers**
  - ▪**Services large bande pour entreprises**
- ➢**Services "co-positionnés" avec les transmissions TV**



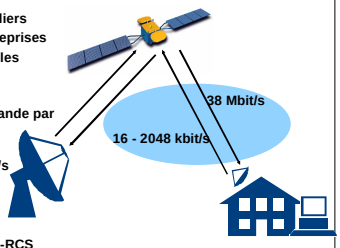
Services à large bande par satellite

▲ **Distribution de services à voie unique avec voie de retour terrestre**

- ➢**Services**
  - ▪**ADSL par satellite pour particuliers**
  - ▪**Services large bande pour entreprises**
- ➢**Services "co-positionnés" avec les transmissions TV**

▲**Services bi-directionnels à large bande par satellite**

- ➢**Panoplie complète de services, avec voie retour de 16 – 2048 kbit/s**
  - ▪**Marché résidentiel: Gilat 360**
  - ▪**PME/SOHO:**
    - **Gilat Skystar Advantage**
    - **BBI, basé sur standard DVB-RCS**



Satellites

Accès à Internet ADSL
large bande tout IP

Source Infosat

Couverture

- Satellite garantit un haut débit sur un grand territoire sans zone d'ombre
- Contrainte : vue dégagée au sud
- Service bidirectionnel large bande norme DVB-RCS

Une technologie DVB RCS « TOUT IP »

- Technologie DVB-RCS
  - DVB MPE Descendant
  - DVB RCS montant
  - Sortie Ethernet
  - Tout IP
    - RIP,IGMP,RTP,UDP,TCP
  - Jusqu'à 60 Mb (desc)
  - Jusqu'à 1,2 Mb (mon)
  - turbo codage
- Technologie VSAT
  - Propriétaire desc.
  - Propriétaire montant
  - Sortie Synchrone ou USB nécessite un routeur
  - Pas de multicast
  - Jusqu'à 8 Mb (desc)
  - Jusqu'à 512kb (mon)

Cadre réglementaire

- Pas de permis de construire (parabole de 95 cm)
- Pas d'autorisation ART (puissance de 2 watt)
- Pose intégrée par un installateur agréé dans le prix de l'équipement terrestre.
- Utilisation en bande KU (10-11 Ghz)

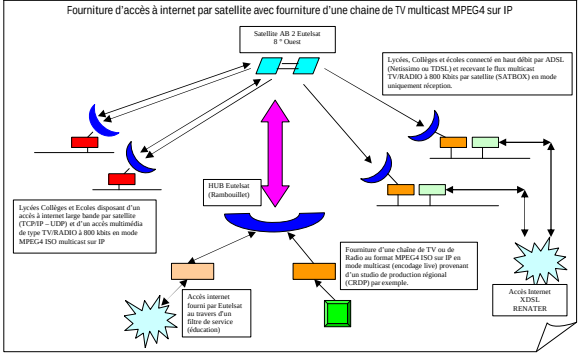
La gestion de qualité de service

- Le DVB RCS permet la gestion de la QOS
  - Gestion de GFU (Group. Fermé d'Utilisateur)
  - Gestion de CIR CBR (montant / descendant)
  - Gestion par adresse MAC (Ethernet)
  - Allocation dynamique de bande passante
  - Gestion multicast à débit garanti pour l'audiovisuel (TV qualité VHS MPEG4 ISO)
  - Gestion QOS au niveau 2

Le multimédia opérationnel

- Disponibilité du multicast sur l'ensemble des stations bi-directionnelles et unidirectionnelles.
- Acheminement de chaînes de TV MPEG4 éducatives sur IP à 800Kb garanti.
- Acheminement de chaîne de radio MPEG4
- Possibilité de lire le flux multicast sur des stations uniquement en réception (DVB MPE)
- Totale interopérabilité avec l'ADSL de F.T.

Exemple de fonctionnement



Des prix performants

- Station bi-directionnelle fournie et installée : 2600 Euros HT
- Une capacité variant selon vos besoins
  - 256/64k 150Euros/mois
  - 512/128 290Euros/mois
  - 768/256 400Euros/mois (offre spécifique)
  - 1024/256 560Euros/mois
  - Chaîne de TV à 650 kbits : 8 750 Euros/mois

Deux acteurs complémentaires

- EUTELSAT SA
- Opérateur transport
  - 1er opérateur européen avec plus de 20 satellites en orbite
  - Des téléports secourus
  - Supervision 24/24
  - Opérateur de TPS
- INFOSAT ICPS SA
- Opérateur de services
  - Premier fournisseur de solution MPEG4 ISO sur IP/DVB
  - 6 ans de R&D sur l'IP/DVB
  - Spécialiste des services IP/DVB

Distribution WiFi en milieu rural

- (3 à 5 Km)
- 1 Hub 3 Mbits sur point haut
- 8 Prises 8 adresses par site (8 entreprises avec 8 postes chacun)
- 1 Station émission/réception satellite

- TOTAL : 25 000 Euros
- Prix de la prise : 3125 Euros

Fonctionnement mutualisé

- Investissement 25 000 Euros sur 3 ans pour 8 prises à 2 Mbits + station satellite
- Amortissement 3 ans : 87 E/mois/prise
- Accès internet satellite 1M/256K :560 E/mois
- Prix total d'une prise avec internet : 157 Euros/mois/prise
- Au delà de 3 ans : 70 € par mois

Projet Satellite + WiFi France Telecom

La question de la couverture haut débit

Pourquoi le haut débit partout ?

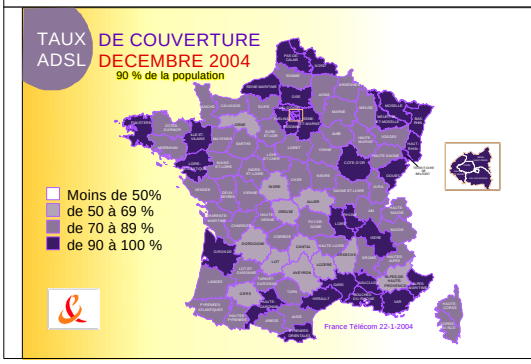
- Pour apporter aux grandes entreprises des solutions hauts débits disponibles et homogènes sur tous leurs sites,
- Pour permettre aux entreprises de poursuivre leur développement en restant sur leurs zones d'activité respectives,
- Pour donner la possibilité aux collectivités locales d'attirer de nouvelles entreprises sur les territoires de leur responsabilité,
- Pour poursuivre le développement du marché haut débit sur l'ensemble du territoire national en collaboration avec les collectivités locales.

Point sur la couverture haut débit

La progression de la couverture haut débit :

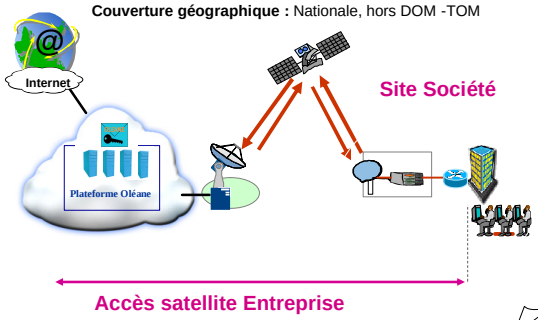
- Fin 2003, une couverture ADSL globale de 79% de la population,
- Dès fin 2004, ce taux de couverture passera à 90 %,
- Discussions avec l'ensemble des acteurs concernés par l'aménagement du territoire pour permettre d'atteindre 95 % de couverture de la population dès fin 2005,
- Développement de solutions complémentaires à l'ADSL avec des technologies alternatives (satellite et WiFi) pour aller à 100 %.

Prévision du taux de couverture ADSL fin 2004



Architecture générale

Couverture géographique : Nationale, hors DOM -TOM



La gamme des accès satellites Entreprises

- Une connexion illimitée à l'Internet Haut Débit en tout point du territoire
  - ❑ Accès 128/64 kb/s
  - ❑ Accès 512/128 kb/s
  - ❑ Accès 1024/256 kb/s
  - ❑ Accès 2 M/ 512 kb/s
- Un service de messagerie
- Une adresse IP fixe
- Un service d'assistance
- Une supervision du réseau de collecte 7j/7 et 24h/24

Le terminal satellite Entreprise

- Fourniture du service : raccordement du site client au réseau IP de France Télécom grâce à l'installation d'un modem-routeur chez le client et d'une antenne satellite orientée vers le sud

Les accès satellites Entreprises : Pack surf Satellite

- **Solution entrée de gamme comprenant les prestations suivantes :**
  - **Une connexion permanente à l'Internet via le satellite** bidirectionnelle 24h/24.
  - Le raccordement du site client au réseau IP de France Télécom s'effectue grâce à l'installation chez le client d'un modem-routeur (IDU) et d'une antenne satellite (ODU) dont le diamètre est de 75 cm à 1,20m orientée vers le Sud.
- **Tarifs :**

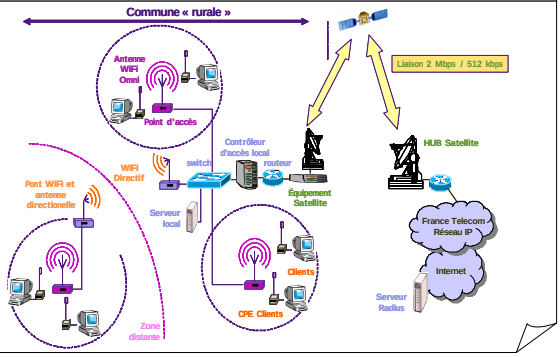
	Accès 1	Accès 2	Accès 3
Débit crête descendant	128 Kbit/s	512 Kbit/s	1 Mbit/s
Débit crête montant	64 Kbit/s	128 Kbit/s	256 kbit/s
Nb de postes conseillés	5	10	20
Terminal à l'achat (€ HT)	1599	1599	1599
FAS	690	690	690
Redevance mensuelle	95	140	250

⇨ Le 2 M/512 Kbit/s est disponible

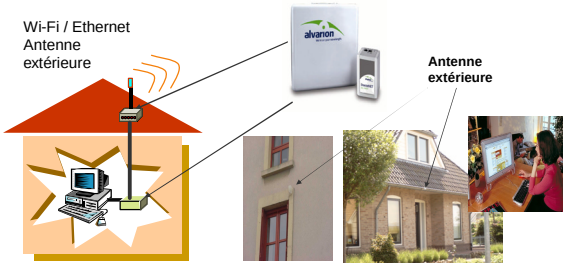
Les accès satellites Entreprises : Oléane Open Sat

- Une messagerie au nom personnalisé,
- Le site web hébergé au nom de l'entreprise :
  - La vitrine sur internet à l'adresse société.com
- Les salariés restent connectés, même en déplacement :
  - Consultation et envoi des messages internet sur mobile WAP/GPRS Orange ou PC portable
  - Envoi et réception des fax à distance avec Fax in Mail
- Mise à votre disposition des outils de productivité collective
  - Gestion des fax et SMS en un seul clic comme les emails, avec Fax in Mail
  - Partage des agendas, des documents et des ressources au sein d'une équipe, y compris avec des partenaires, grâce à Bizao

Pack Surf Wi-Fi : comment ça marche ?



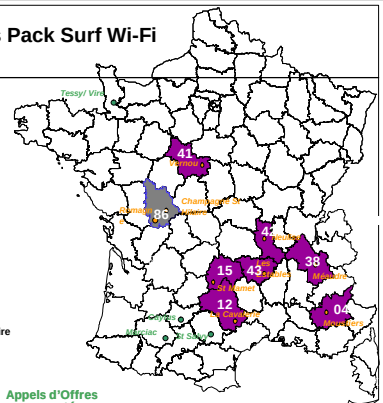
L'équipement client



Les déploiements Pack Surf Wi-Fi

Expérimentations « Pack Surf WiFi »

La Cavalerie (12)
Inauguration le 2 Octobre
Méaudre (38)
Inauguration le 3 Novembre
Moustier-St-Marie (04)
Inauguration le 7 Novembre
Neulise (42)
Inauguration le 23 Octobre
Vernou-en-Sologne (41)
Inauguration le 24 Novembre
Saint Mamet (15)
Inauguration le 15 décembre
Estables (43),
Inauguration le 19 février
Romagne (86), Champagné Saint Hilaire (86)
Inauguration le 9 mars 2004



Appels d'Offres remportés

Les expérimentations Pack Surf WiFi

Contexte :

9 sites expérimentaux, dont les inaugurations s'échelonnent de début octobre 2003 à mars 2004

Investissements et installation pris en charge par France Telecom

Une architecture homogène pour l'ensemble des sites : accès satellite 2 Mo, un routeur, 3 cellules, un contrôleur d'accès.

Les offres proposées aux clients finaux :

128/64 Kbit/s, 256/64 Kbit/s et 512/64 Kbit/s,

Des offres packagées comprenant la connectivité internet et un service de boîte aux lettres,

Des services locaux : Tableau virtuel et notification d'événements.

Bilan des expérimentations Pack Surf WiFi

- **144 clients raccordés , sur 7 sites ouverts**
- **Taille moyenne des communes : 790 habitants**
- **21 clients par commune en moyenne, soit un taux de pénétration moyen : 3%**
  - **50% Résidentiel**
  - **50% Pros, PME, collectivités**

Répartition des placements :

- **128/64 : 60%,**
- **256/64 : 32%**
- **512/128 : 8 %**

Boucle Locale Radio (BLR)

Point sur les licences : source TACTIS

Sommaire

1 – Enjeux : Concurrence sur l'accès à l'abonné

- Boucle locale télécom : marché en situation de quasi monopole (opérateur historique dominant, avec peu de réseaux câblés offrant des services télécoms et un nombre limité de boucles locales optiques)
- Un marché estimé par l'ART à 56 milliards de francs en 1999
  - dont 32 milliards pour l'abonnement
  - 24 milliards pour les communications locales (dont plus de 2 milliards uniquement pour l'accès Internet)
- Atouts de la BLR :
  - Solution rapide pour ouvrir la boucle locale à la concurrence, début 2001
  - Coût d'installation estimé à 40% inférieur à celui d'un réseau fixe
  - Investissement progressif pour les opérateurs (station de base, station terminale)
  - Des capacités de débits supérieures au technologies filaires cuivres actuelles

2.1 - Deux Licences BLR Nationales

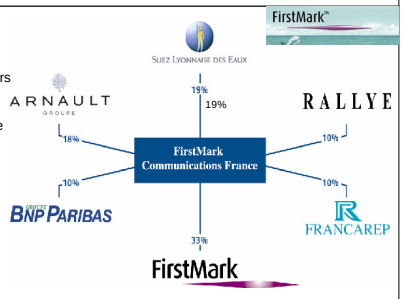
- Firstmark Communications France
- Fortel

Candidats retenus	Licences demandées	Licences attribuées
Firstmark Communications France	1 nationale, 22 régionales	1 nationale
Fortel	1 nationale, 11 régionales	1 nationale
Candidats non retenus	**Licences demandées**	**Licences attribuées**
Cegetel	1 nationale, 2 DOM	2 DOM (Guadeloupe - Martinique, La Réunion)
Siris	1 nationale, 22 régionales	2 régionales (Auvergne, Corse)
Skyline	1 nationale, 11 régionales	aucune
Tele2 BLR	1 nationale	aucune
9 telecom Réseau	1 nationale	aucune
Winstar	1 nationale, 12 régionales	aucune

Firstmark Communications France

•Capital

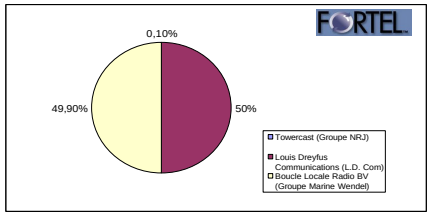
FirstMark Communications France est un consortium rassemblant quelques ténors comme le Groupe Arnault, Suez-Lyonnaise des Eaux (candidate pour une licence UMTS en France), BNP-Paribas, Rothchild…



Fortel

•Capital

Fortel est un consortium rassemblant Marine Wendel contrôlés par Ernest-Antoine Sellière, la société Louis Dreyfus Communications (L.D. Com) remplaçant le cablo-opérateur UPC, et le groupe de radio NRJ par le biais de sa filiale Towercast. A noter, la société L.D.Com, est également actionnaire à hauteur de 50,1 % de la société BLR Services



Les investissements prévisionnels des deux opérateurs nationaux

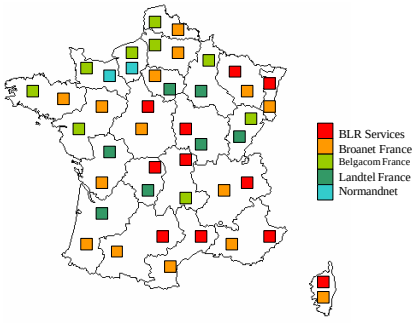
	Firstmark Communications	Fortel
Investissements cumulés prévisionnels sur l'ensemble des deux bandes en 2004		
Investissements dans les stations de base	1 000 MF	1 400 MF
Investissements dans les liaisons point à point	625 MF	1 250 MF
Investissements dans les équipements devant être installés chez les clients	300 MF	8200 MF (Les antennes de réception grand public environ 5 000 Frs pièce - devraient être mises gratuitement à disposition des clients)
Total des investissements cumulés	2 000 MF	11 000 MF (17 000 MF sur 10 ans selon les engagements pris dans le dossier de candidature et 3 à 4 Milliards si l'on se réfère aux déclarations (7 août 2000) de Patrick DAHI, président du directoire de Fortel)
Coût moyen de la station de base	1,10MF	0,97MF

2.2 – Licences Régionales : 7 opérateurs retenus

- 7 retenus sur 18 candidats métropolitains et 197 dossiers régionaux

Candidats retenus	Licences demandées	Licences attribuées
Altitude	2 régionales	**2 régionales**
Belgacom France	13 régionales	**7 régionales**
BLR Services (LDCOM), ex Proximus	14 régionales	**8 régionales**
Broadnet France SAS	15 régionales	**14 régionales**
Completel	18 régionales	**4 régionales**
Landtel France	17 régionales	**7 régionales**
Siris	1 nationale, 22 régionales	**2 régionales**
Candidats non retenus	**Licences demandées**	**Licences attribuées**
Estel	1 régionale	**aucune**
IS Production	1 régionale	**aucune**
Kast Telecom	7 régionales	**aucune**
Telecontinent SA	6 régionales	**aucune**
NTL France SAS	2 régionales	**aucune**
Formus Communications France SAS	10 régionales	**aucune**
Kapstar	12 régionales	**aucune**
Skyline	1 nationale, 11 régionales	**aucune**
Winstar	1 nationale, 12 régionales	**aucune**
Firstmark	1 nationale,22 régionales	**1 nationale**
Fortel	1 nationale,22 régionales	**1 nationale**

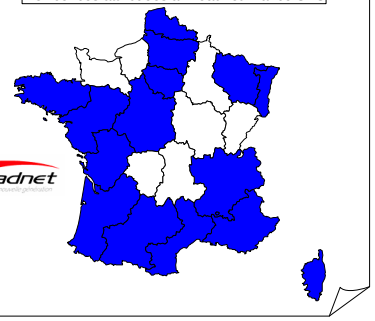
Carte des opérateurs régionaux de BLR



Les 7 lauréats à l'attribution des licences régionales

- BROADNET France SAS
- Capital :
  - Broadnet Holding BV (90%) (groupe Comcast – USA)
  - Axa (10%)

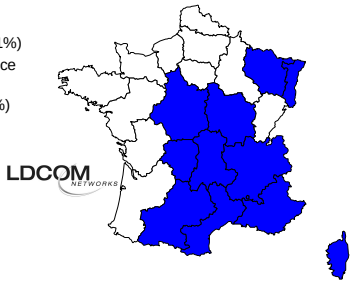
15 licences attribuées à Broadnet France SAS



Les 7 lauréats à l'attribution des licences régionales

- BLR SERVICES LDCOM
- Capital :
  - LDCOM (50,1%)
  - Teligent France (40%)
  - Artemis (9,9%)

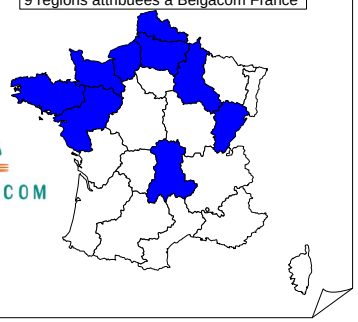
11 régions attribuées à BLR Services (LDCOM)



Les 7 lauréats à l'attribution des licences régionales

- BELGACOM FRANCE
- Capital :
  - Belgacom (100%)

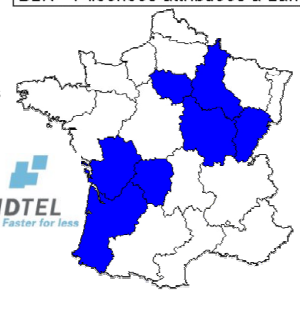
9 régions attribuées à Belgacom France



Les 7 lauréats à l'attribution des licences régionales

- LANDTEL FRANCE
- Capital :
  - Landtel N.V. à 100% elle même filiale à 100% de Landover Holdings Corp (LHC) - USA

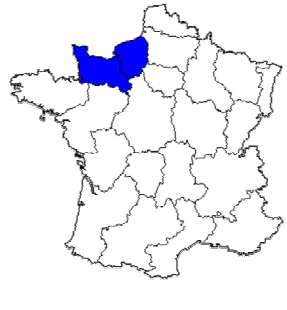
BLR - 7 licences attribuées à Landtel France



Les 7 lauréats à l'attribution des licences régionales

- ALTITUDE
- Capital :
  - M. Jean-Paul Rivière quasiment à 100%

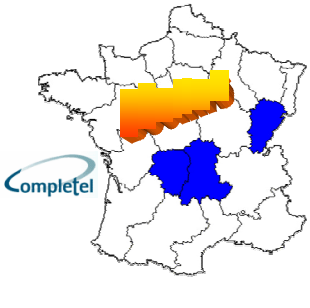
BLR - Deux régions attribuées à ALTITUDE



Les 7 lauréats à l'attribution des licences régionales

- COMPLETEL
- Capital :
  - Completel Europe (100%) elle même filiale de Completel USA à 100%
- L'ART a attribué ces quatre régions à d'autres opérateurs suite au désistement de Completel.

BLR - 4 licences attribuées à Completel

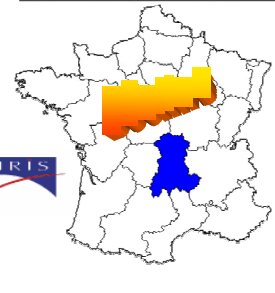


Les 7 lauréats à l'attribution des licences régionales

- SIRIS
- Capital :
  - Deutsche Telekom (100%)

L'ART a attribué ces deux régions à d'autres opérateurs suite au désistement de Siris.

BLR - 2 régions attribuées à Siris



2.3 - Département d'Outre Mer : 3 opérateurs

- Trois « opérateurs » obtiennent 8 licences (sur 5 candidats / 13 dossiers)

Candidats retenus	Licences demandées	Licences attribuées
Cegetel (Cegetel Caraïbes SA, Cegetel La Réunion SA	1 nationale, (2+1) DOM	**3 DOM** (Guadeloupe - Martinique - La Réunion)
XTS Network (XTS Network Caraïbes, XTS Network Océan Indien)	(3+1) DOM	**4 DOM** (Guadeloupe - Martinique - La Réunion - Guyane)
Informatique Télématique SA		**1 DOM** (Guyane)
Candidats non retenus	**Licences demandées**	**Licences attribuées**
Dauphin Telecom	1 Dom	**aucune**
World Satellite Guadeloupe	1 Dom	**aucune**

3 - Objectifs de couverture territoriales des deux opérateurs nationaux de BLR (pour la métropole)

	31/12/01	30/06/03	31/12/04
Engagement en termes de taux de couverture de l'ensemble du territoire métropolitain			
Bande 3,5GHz			
Firstmark Communications	20,70%	32,80%	33,40%
Fortel	30%	41%	46%
Bande 26GHz			
Firstmark Communications	14,50%	22,40%	22,70%
Fortel	21%	29%	31%
Taux de couverture de la population (unité urbaine > 50 000 habitants) et prévision du nombre d'unités couvertes (pour les deux bandes)			
Bande 3,5GHz			
Firstmark Communications	(40)	(127)	58,3% (146)
Fortel	(21)		85%(165)
Bande 26GHz			
Firstmark Communications	(40)	(127)	34,5% (146)
Fortel	(21)		60%(165)

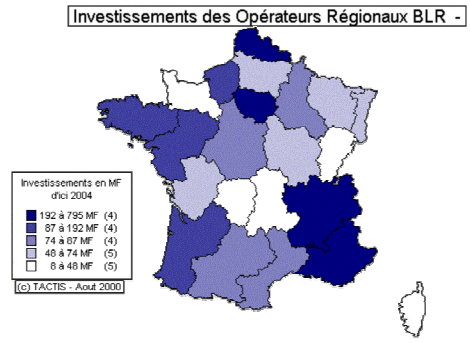
3 - Objectifs de couverture territoriales des deux opérateurs nationaux de BLR (pour la métropole)

BLR opérateurs régionaux : Classement des régions / taux de couverture territoire au

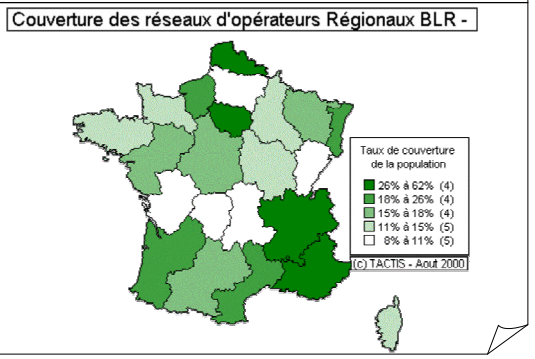
Régions -©TACTIS Aout 2000	Total des investissements cumulés au 31/12/04 en millions de francs	Taux régional de couverture radio.de la population au 31/12/04	Nombre de Clients	Nombre de stations de base
Ile-de-France	795	61,50%	17 887	344
Provence-Alpes-Côte d'Azur	192	35,00%	1 666	166
Rhônes-Alpes	195	33,00%	1 630	179
Nord Pas-de-Calais	105	26,00%	1 530	95
HAUTE-NORMANDIE	92	24,86%	1 441	97
Alsace	55	22,00%	894	37
Languedoc-Roussillon	01	20,00%	732	72
Aquitaine	96	19,00%	2 109	-
Centre	83	16,80%	947	61
Lorraine	52	16,00%	891	44
Midi Pyrenées	75	16,00%	729	62
Pays de la Loire	130	15,00%	1 142	42
Champagne-Ardenne	74	14,50%	1 491	21
Bourgogne	57	14,00%	1 302	37
Basse Normandie	37	13,32%	673	16
Bretagne	87	12,00%	920	28
Corse	8	11,00%	93	8
Picardie	60	10,80%	606	22
Poitou Charentes	48	10,00%	402	26
Franche-Comté	30	9,80%	548	19
Auvergne	18	9,00%	187	11
Limousin	27	8,00%	686	11
Totaux	2 487		37 504	1 348
Opérateurs nationaux		31,03%	157 210	1 276

Pour les deux opérateurs nationaux, la répartition des taux de couverture par région n'est pas publique.

3 - Objectifs de couverture territoriales des deux opérateurs nationaux de BLR (pour la métropole)



3 - Objectifs de couverture territoriales des deux opérateurs nationaux de BLR (pour la métropole)

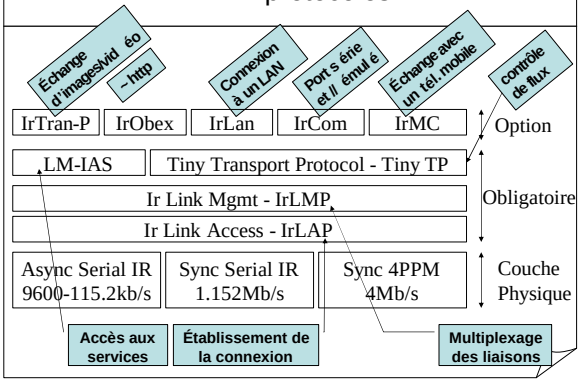


IrDA

Standard IrDA

- Objectifs
  - Réseau personnel : très courte portée ~ 1 mètre
  - Hauts débits : jusqu'à 4 Mbit/s
  - Faible coût, large diffusion dans tous les périphériques
- Création d'un standard : Infrared Data Association (IrDA)

IrDA : protocoles



Caractéristiques couche physique

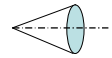
- Transmission de 9,6kb/s à 4Mb/s
- CRC-16 ou CRC-32 (pour le 4Mb/s)
- Chargé de la négociation sur la vitesse
- Paquet HDLC + 2 flags au début

STA	STA	ADDR	DATA	16b FCS	STO

Frame abort : après 7 échecs !!!

Caractéristiques

- Half-duplex : les Full-duplex sont simulés
- Source directionnelle
  Cône de transmission : 2x15°
  Il faut être dans l'axe…

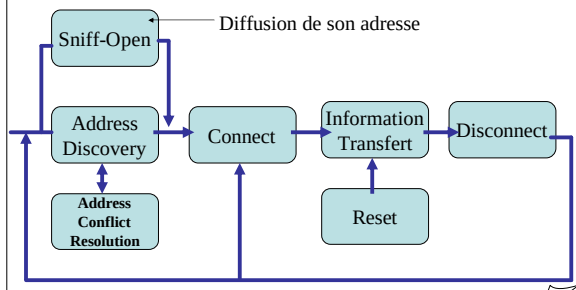


- Point-à-point uniquement
- Pas de détection de collision...
  les protocoles de haut niveau se débrouillent...

IrDA : maître-esclave

- Deux périphériques doivent prendre chacun un rôle (couches basses uniquement) :
  - Primary station : initie la communication par une « command frame » et contrôle le flux entre les deux équipements
  - Secondary station : ne répond que lorsqu'on l'interroge
- Personne ne transmet plus de 500ms

Négociation « services discovery »

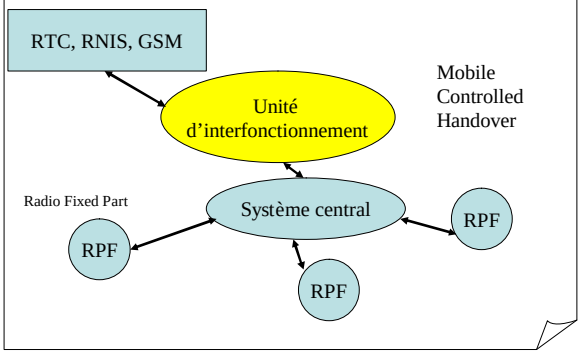


DECT

DECT

Fréquence	1,8-1,9 GHz
Nbre de fréquences	10
Canaux/porteuse	12 Duplex
Assignation canal	Dynamique
Technologie	Numérique
Portée	50-500 m
Séparation porteuse	1,728 MHz
Transmission	TDMA
Puissance porteuse	250 mW
Puissance canal	10 mW
Débit maximal	1,5 Mbits/s
Longueur de trame	10 ms

DECT



WiFi - IEEE 802.11

PLAN

- Définition
- Standard
- Fonctionnalités, architecture
- Sécurité
  - Sécurité de base
  - Les protocoles assurant la sécurité
    - 802.1x
    - 802.11i
  - Sécurisation supplémentaire : IPSec
  - Outils de détection
  - Conclusion : préconisations

Définition

- Le **WI-FI** répond à la norme **IEEE 802.11**. La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN).
- Le nom **Wi-Fi** (contraction de ***Wireless Fidelity***) correspond initialement au nom donnée à la certification délivrée par la WECA (http://www.weca.org/) Etats-Unis (*Wireless Ethernet Compatibility Alliance*), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.
- C'est la Wi-Fi Alliance qui pose le **label** " Wi-Fi " et certifie les produits des constructeurs (+200 sociétés).
- 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. Ainsi un réseau Wifi est en réalité un réseau répondant à la norme 802.11.

Normes IEEE 802.xx

- IEEE : Institute of Electrical and Electronics Engineers

Normes	Définition
802.1	Modèle architectural séparant les deux couches OSI Physique et Liaison en 3 couches : PLS,MAC, LLC
802.2	Norme IEE couche LIAISON
802.3	Norme IEE ETHERNET / CSMA/CD
802.4	Norme IEEE TOKEN BUS (industriel IBM) – Anneau à jetons
802.5	Norme IEEE TOKEN BUS (non propriétaire inspiré d'IBM)
802.6	Norme IEEE de réseau métropolitain à double bus.
802.7	Norme IEEE FDDI (Fiber Distributed Data Interface) – Fibre Optique
802.8	Projet IEEE sur les Fibres Optiques / Résilié le 11/09/2002
802.9	Norme IEEE Integrated Service LAN (ISLAN)
802.10	Norme IEEE de sécurité réseau 802 (SILS : Standard for Interoperable Lan Security)
802.11	Série de normes IEEE pour réseau local sans fil

Standards IEEE 802.11

- **802.11** : L'ancêtre du réseau sans fil, sur 2,4 GHz modulation DSSS ou saut de fréquence (aucune norme imposée), d'un débit de 2 Mb/s et pratiquement pas inter-opérable de constructeur à constructeur.
- **802.11b** : premier réseau Ethernet sans fil interopérable, sur 2,4 GHz, offrant un débit physique de 11 Mb/s (modulation DSSS, accès par CSMA/CA et détection de porteuse)
- **802.11a** : (baptisé WiFi 5) historiquement c'est le second projet de réseau Ethernet sans fil sur 5 GHz, elle permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). Pas de compatibilité avec 802.11b
- **802.11g** : est la norme la plus répandue actuellement. Adaptation d'OFDM aux réseaux 802.11b (compatibilité) (passage à 54 Mb/s). La norme 802.11g a une compatibilité ascendante avec la norme 802.11b.

Standards IEEE 802.11

- **802.1x** : Sous-section du groupe de travail 802.11i visant à l'intégration du protocole EAP (authentification) dans les trames Ethernet (indépendamment de tout protocole PPP, contrairement aux accès RAS conventionnels). 1x permet l'usage d'un serveur d'authentification de type Radius.
- **802.11i** : Amélioration au niveau MAC destinée à renforcer la sécurité des transmissions, et se substituant au protocole de cryptage WEP (Wired Equivalent Privacy).

  En cours de finalisation

Standards IEEE 802.11

- **802.11c** : Complément de la couche MAC améliorant les fonctions « pont », reversé au Groupe de Travail 802.11d
- **802.11d** : Adaptation des couches physiques pour conformité aux exigences de certains pays particulièrement strictes (essentiellement la France et le Japon)
- **802.11e** : Complément de la couche MAC apportant une qualité de service aux réseaux 802.11a, b et g. Norme en voie d'achèvement
- **802.11f** : Document normatif décrivant l'interopérabilité inter constructeurs au niveau de l'enregistrement d'un point d'accès (AP) au sein d'un réseau, ainsi que les échanges d'information entre AP lors d'un saut de cellule (roaming). Norme en voie d'achèvement

Standards IEEE 802.11

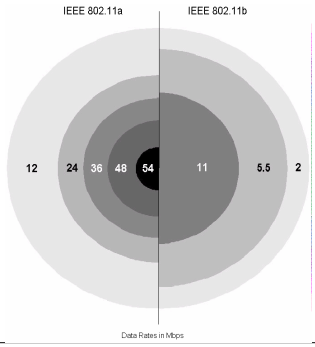
- **802.11h** : Amélioration de la couche MAC visant à rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2.

  802.11h s'occupe notamment de l'assignation automatique de fréquences de l'AP et du contrôle automatique de la puissance d'émission, visant à éliminer les interférences entre points d'accès. En cours d'élaboration, travail commun entre l'IEEE et l'ETSI .

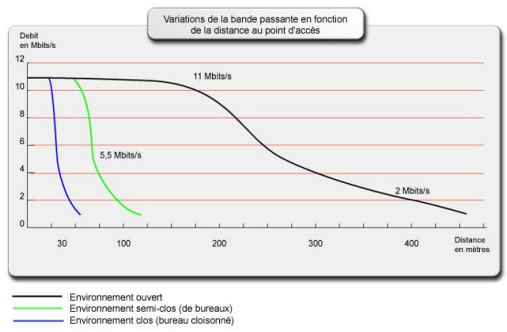
Standards les plus courants IEEE 802.11

Norme	Année	Débit Mb/s	Bande GHz	
802.11a	1999	6; 9; 12; 18; 24; 36; 48; 54	5	
802.11b	1999	11	2,4	
802.11g	2001-2003	54	2,4	Compatibilité ascendante 802.11b

Débits en fonction de la distance 802.11a/b



Débits en fonction de la distance 802.11b



Usages

Réseaux ouverts au public dans le cadre de projet de développement local

- Les implantations sont possibles partout depuis 25 juillet 2003 - Déclaration à ART uniquement demandée
- Toute installation extérieure n'est plus soumise à une autorisation préalable fournie par l'ART (Autorité des Réseaux et Télécommunications). Toutefois, la déclaration est obligatoire.

Bornes d'accès WI-FI dans les lieux dits de passage : "Hot Spots"

- Lieux de passage à forte influence, tels que les aéroports, les gares, les complexes touristiques, bars, hôtels …
- Pas d'autorisation lorsqu'elles sont raccordées directement à un réseau ouvert au public existant (en général un opérateur de télécommunications).
- Les opérateurs télécoms et autres FAI proposent des abonnements, à durée limitée (5€ pour 20 minutes, 10 à 20 € pour 2 heures selon l'opérateur) ou illimitée pendant une période donnée (30€ pour 24 heures)

IEEE 802.11 : Fonctionnalités

- **Architecture cellulaire** : des stations mobiles utilisent des stations de base (points d'accès) pour communiquer entre eux.
- Un réseau Wi-Fi est composé de un ou plusieurs **points d'accès** avec plus ou moins de stations mobiles équipées de cartes Wi-Fi.
- **Taille du réseau** : dépend de la zone de couverture du point d'accès, aussi appelé cellule.
- **Une cellule unique** constitue l'architecture de base de Wi-Fi, appelée BSS (Basic Service Set), ou ensemble de services de bases.
- **Roaming :** Déplacement d'une cellule (BSS) à une autre
- **Handover** : Mécanisme qui permet de se déplacer d'une cellule à l'autre sans interruption de la communication.

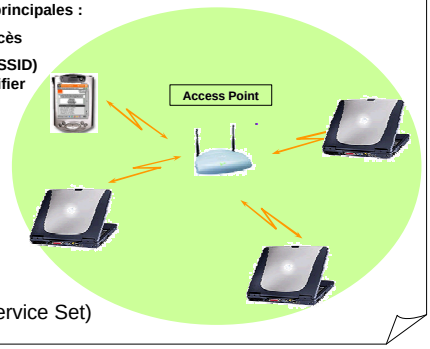
IEEE 802.11 : Architecture

- Il existe deux types de topologies :
  - Le **mode infrastructure**, avec **BSS** et **ESS**.
    - En mode infrastructure **BSS**, le réseau est composé d'un point d'accès qui permet aux différentes stations qui se trouvent dans sa cellule d'échanger des informations.
    - En mode infrastructure **ESS**, le réseau comporte plusieurs points d'accès reliés entre eux par un DS
  - Le **mode ad-hoc**
    - En mode ad-hoc, ne comporte pas de points d'accès, ce sont les stations (avec cartes Wi-Fi) qui entrent elles mêmes en communication.

IEEE 802.11 : Architecture BSS

Caractéristiques principales :

- **1 seul point d'accès**
- **Nom de réseau (SSID) Service Set IDentifier**

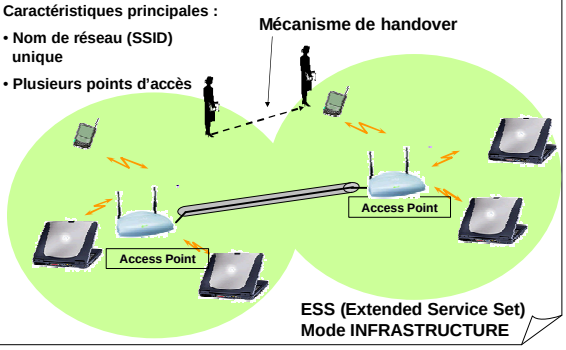


BSS (Basic Service Set)

IEEE 802.11 : Architecture ESS et handover

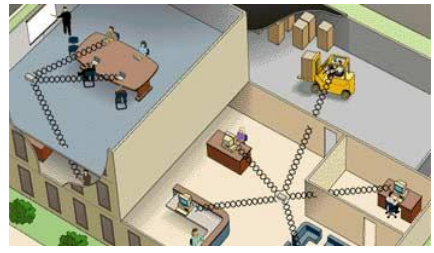
Caractéristiques principales :

- **Nom de réseau (SSID) unique**
- **Plusieurs points d'accès**



ESS (Extended Service Set)
Mode INFRASTRUCTURE

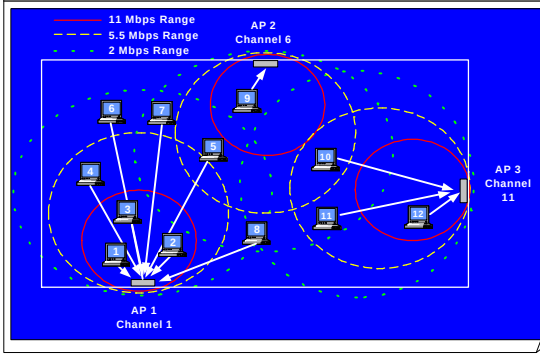
IEEE 802.11 : Architecture ESS



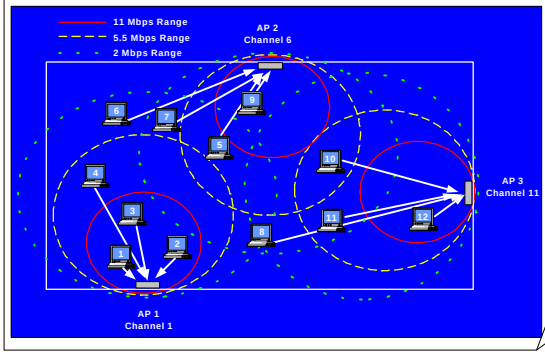
IEEE 802.11 : Architecture ESS

- La station client recherche toujours le meilleur débit
- Les points d'accès contrôlent la charge et peuvent autoritairement terminer l'association avec une station client

Répartition dynamique de charge : **avant**



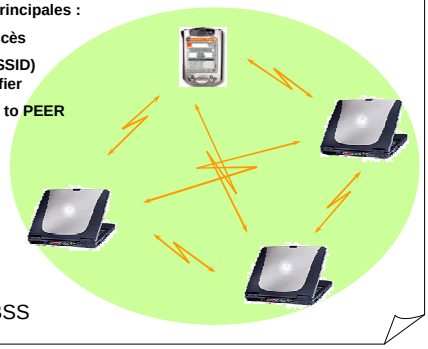
Répartition dynamique de charge : **après**



IEEE 802.11 : Architecture IBSS (Mode ad'hoc)

Caractéristiques principales :

- **Pas de point d'accès**
- **Nom de réseau (SSID) Service Set Identifier**
- **Topologie : PEER to PEER**

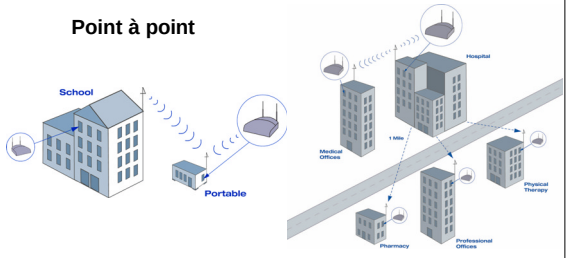


Independant BSS

Pont radio

Point à multipoints

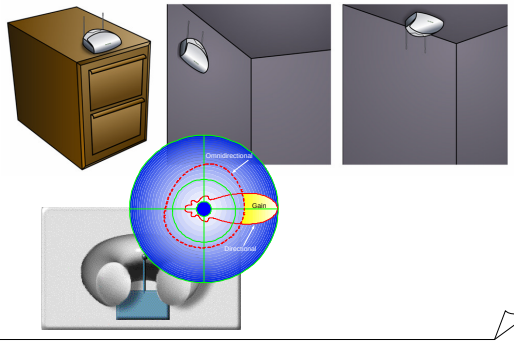
Point à point



Matériel

- Éléments actifs
  - Point d'accès
  - Bridge
  - Point to Multipoint
  - AP Client
- Éléments passifs
  - cartes clientes (PCMCIA, PCI, USB)
  - antennes

Antennes : orientation



802.11 Modèle OSI

Couche liaison de données	LLC 802.2			
	MAC 802.11, sécurité, etc …			
Couche physique	FHSS	DSSS	IR	OFDM

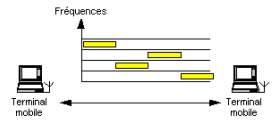
- FHSS : étalement de spectre par saut de fréquence
- DSSS : étalement de spectre en séquence directe
- IR : InfraRouge
- OFDM : Multiplexage en fréquences

IEEE 802.11

Couche physique

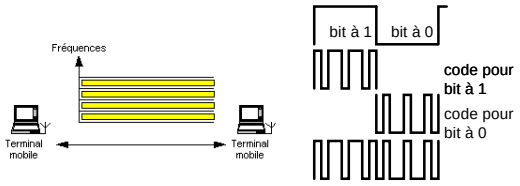
FHSS : étalement de spectre par saut de fréquence

- FHSS (Frequency Hopping Spread Spectrum) : consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule.
- Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée.



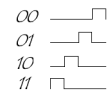
DSSS : étalement de spectre à séquence directe

- DSSS (Direct Sequence Spread Spectrum) : consiste à transmettre pour chaque bit une séquence (11bits) . Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.



InfraRouge

- Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge :
  - utilise une onde lumineuse pour la transmission de données.
  - uni-directionnelle, soit en "vue directe" soit par réflexion
  - offre un niveau de sécurité plus élevé (caractère non dissipatif des ondes lumineuses)
- Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelée PPM (pulse position modulation).
- le débit de 2 Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles



OFDM (Orthogonal Frequency Division Multiplex)

- Principe : diviser le canal principal en sous canaux de fréquence plus faible.
  Chacun de ces sous canaux est modulé par une fréquence différente, l'espacement entre chaque fréquence restant constant. Ces fréquences constituent une base orthogonale : le spectre du signal OFDM présente une occupation optimale de la bande allouée.
- Multiplexage en fréquences

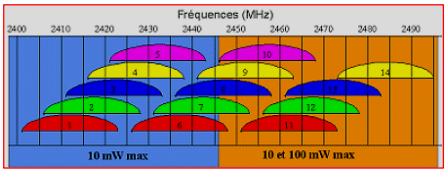
Types de modulation

- PSK (Modulation de phase)
- QPSK (Modulation de phase en quadrature)
- CCK (Complementary Code Keying)
  Symboles de m bits codés par une séquence de m bits (codes orthogonaux complexes)

Technologie	Codage	Type de modulation	Débit
802.11b	DSSS (11 bits)	PSK	1Mbps
802.11b	DSSS (11 bits)	QPSK	2Mbps
802.11b	CCK (4 bits)	QPSK	5.5Mbps
802.11b	CCK (8 bits)	QPSK	11Mbps
802.11a	CCK (8 bits)	OFDM	54Mbps
802.11g	CCK (8 bits)	OFDM	54Mbps

Bande ISM (Industrial, Scientific and Medical)

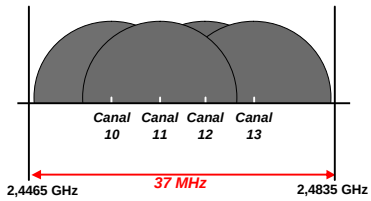
- Bande ISM
  - Bande divisée en 14 canaux de 20 MHz
  - Problème de recouvrement
  - Superposition de 3 réseaux au sein d'un même espace
  - Largeur de bande 83 MHZ



Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Fréquence (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

Bande ISM

"Pays"	États-unis	Europe	Japon	France
Nombres de sous-canaux utilisés	1 à 11	1 à 13	14	10 à 13



802.11b - Portée

- Bande ISM
- Basé sur le DSSS
- Débits compris entre 1 et 11 Mbits/s
- Variation de débits selon la qualité de l'environnement radio (murs, meubles, interférences, distance des équipements, micro-ondes …)

à l'intérieur		à l'extérieur	
Vitesse Mbits/s	Portée (en m)	Vitesse Mbits/s	Portée (en m)
11 Mbits/s	50 m	11 Mbits/s	200 m
5,5 Mbits/s	75 m	5,5 Mbits/s	300 m
2 Mbits/s	100 m	2 Mbits/s	400 m
1 Mbits/s	150 m	1 Mbits/s	500 m

Bande UN-II (5GHz)

- Bande divisée en 8 canaux de 20 MHz
- Pas de problème de recouvrement (atténuation du bruit)
- Co-localisation de 8 réseaux au sein d'un même espace
- Largeur de bande 200 MHZ

Canal	36	40	44	48	52	56	60	64
Fréquence (GHz)	5,18	5,20	5,22	5,24	5,26	5,28	5,30	5,32

Bande UN-II - Réglementation

- En France

Fréquence en MHZ	Intérieur	Extérieur
5150 - 5250	200 mW	impossible
5250 - 5350	200 mW ou 100 mW	impossible
5470 - 5725	impossible	impossible

802.11a - Portée

- Bande UN-II (5GHz)
- Largeur de la bande : 200 MHz
- Basé sur OFDM
- Débits compris entre 6 et 54 Mbits/s
- Pas de compatibilité avec 802.11b

à l'intérieur	
Vitesse Mbits/s	Portée (en m)
54	10
48	17
36	25
24	30
12	50
6	70

802.11g

- Très bon compromis entre 802.11b et 802.11a
- Bande ISM
- Basé sur OFDM et DSSS
- Débits compris entre 6 et 54 Mbits/s
- Compatibilité ascendante avec 802.11b

- La bande ISM est de plus en plus saturée (802.11b, 802.11g, Bluetooth, etc.)

IEEE 802.11

Couche Liaison

Couche Liaison de données

Couche liaison de données	**LLC 802.2 Contrôle de liaison logique**
	MAC 802.11, sécurité, etc … Contrôle d'accès au support

- La couche MAC définit 2 méthodes d'accès différentes
  - La méthode CSMA/CA utilisant la Distributed Coordination Function
  - La Point Coordination Function (PCF) : voix, vidéos …
- La couche MAC offre 2 mécanismes de robustesse :
  - sommes de contrôle (CRC sur 32 bits)
  - fragmentation des paquets

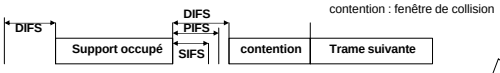
Méthode d'accès

- **Rappel** : dans un réseau **éthernet** filaire, utilisation de la méthode d'accès **CSMA/CD** (**Carrier Sense Multiple Access with Collision Detection**)
- Pour un environnement sans fil : utilisation **CSMA/CA** (**Carrier Sense Multiple Access with Collision Avoidance**) commun aux 3 normes : a, b et g, car :
  - 2 stations communiquant avec un récepteur (AP) ne s'entendent pas forcément mutuellement en raison de leur rayon de portée.
  - Caractéristique : utilise un mécanisme d'esquive de collision basé sur un principe d'accusés de réception (**ACK**) réciproques entre l'émetteur et le récepteur
  - Gère très efficacement les interférences et autres problèmes radio
  - Deux méthodes d'accès au canal basées sur CSMA/CA ont été implémentées pour les réseaux 802.11 : **DCF** et **PCF**

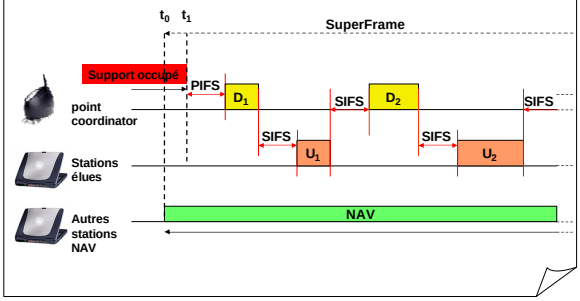
Méthode d'accès

CSMA/CA est basé sur :

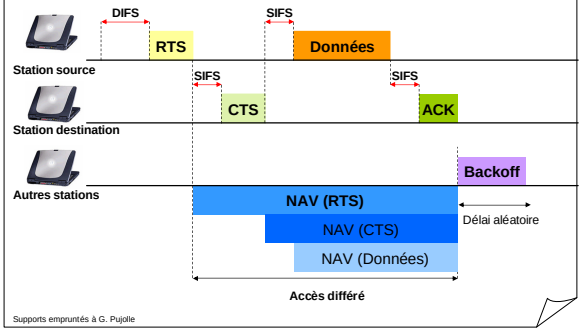
- L'écoute du support :
  - Mécanisme de réservation du support (Ready To Send /Clear To Send)
  - Network Allocation Vector (NAV)
- Les temporisateurs IFS (Inter Frame Spacing)
  - SIFS (Short IFS) : Plus haute priorité pour ACK, CTS interrogations en PCF
  - PIFS (PCF IFS) : Priorité Moyenne, pour le PCF, service en temps réel
  - DIFS (DCF IFS) : Priorité Faible pour le DCF
- L'algorithme de Backoff
- L'utilisation d'acquittement positif



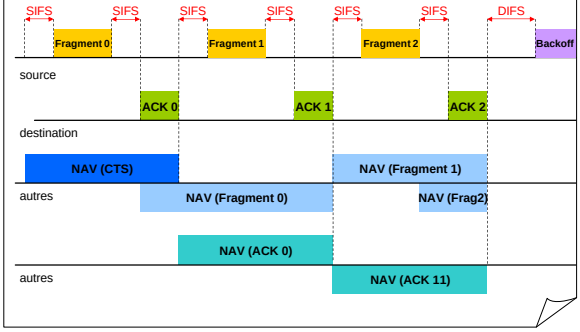
PCF (Point Coordination Function)

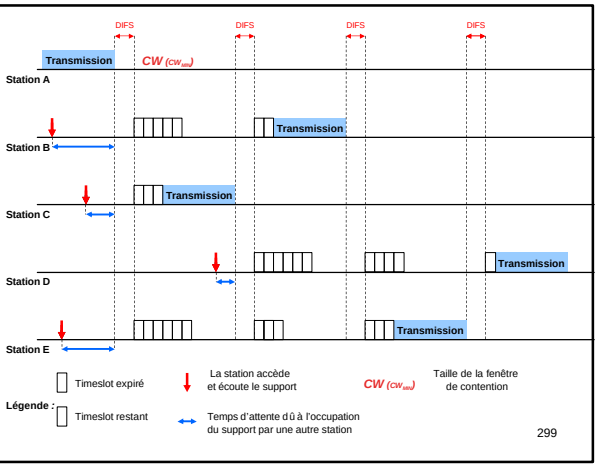


DCF (Distributed Coordination Function)

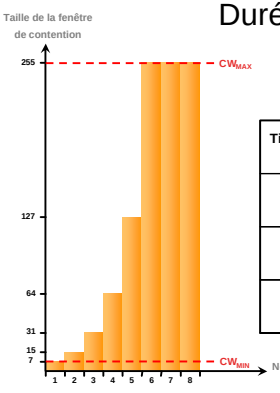


Supports empruntés à G. Pujolle





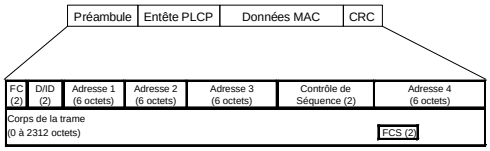
Durées



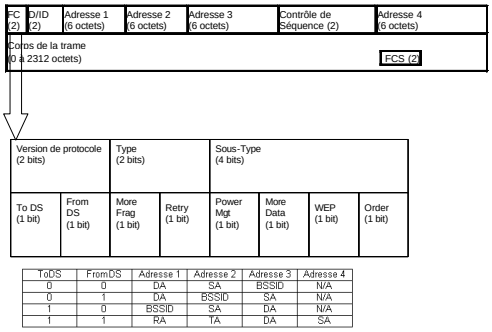
	FHSS	DSSS	IR
Timeslot (µs)	50	20	8
SIFS (µs)	28	10	7
DIFS (µs)	128	50	19
PIFS (µs)	78	30	15

Trames 802.11

- 3 types de trames :
  - trames de données
  - trames de contrôle (contrôle d'accès au support : RTS/CTS)
  - trames de gestion (échange d'informations de gestion)



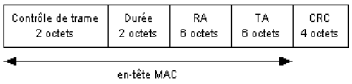
Trame de données 802.11



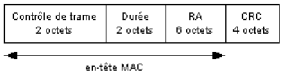
ToDS	FromDS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Trame de contrôle 802.11

Format **RTS**



Format **CTS**



Format **ACK**

IEEE 802.11

Sécurité

Sécurité

- Le problème de sécurité du sans fil : le support de transmission est l'air
  - ➢Des "prises" du réseau sont à disposition pour toute personne à l'intérieur voire à l'extérieur du site (zone couverte par le réseau sans fil).
- 4 types d'attaques :
  - Interception de données, écoute clandestine
  - Intrusion réseau (intrusion, usurpation)
  - Le brouillage radio
  - Les dénis de services

Les attaques : brouillage radio

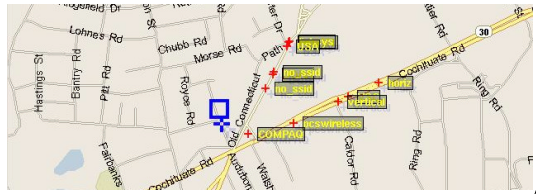
- **Brouillage radio**
  - Création de système radio générant du bruit dans la bande des 2,4GHz. (utilisation de système utilisant la même bande de fréquence : téléphone …)

Les attaques : refus de service

- **Deny of service**
  - Génération de trafic à travers le point d'accès vers un serveur.
  - Installation d'un point d'accès «malicieux» pour détourner le trafic.

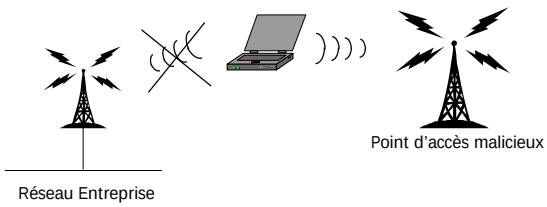
Les attaques : écoute clandestine

Un jeu : le **War Driving** = Quadrillage d'une ville avec
- ✓un ordinateur portable ou un PDA ,
- ✓une carte 802.11 et une antenne externe
- ✓un récepteurs GPS pour la localisation.



Les attaques : intrusion sur le réseau

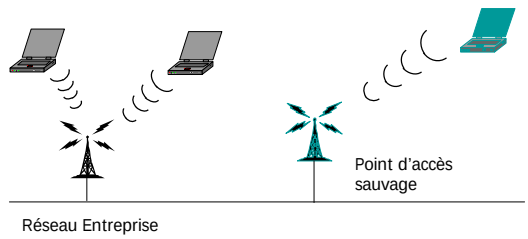
- Point d'accès «malicieux»



Il suffit de connaître le SSID du réseau et le client s'associe au point d'accès «malicieux»

Les attaques : intrusion sur le réseau

- Point d'accès sauvage



La sécurité de base avec 802.11

- Réglage de la puissance d'émission des bornes (Étude du rayonnement des cellules)
- Désactivation des services d'administration disponibles
- SSID :
  - changement de SSID par défaut
  - désactivation du Broadcast du SSID
- Filtrage d'adresse MAC :
  - utilisation des ACL (Access LISTS) des clients RLAN au niveau des bornes d'accès
- Utiliser la Clé WEP (64 bits / 128 bits) et modifier la clé par défaut

Protections de base très peu utilisées !!!

L'authentification par le SSID

- Le **SSID** (**Service Set Identifier**):

  Le client et le point d'accès doivent avoir le même SSID pour s'associer.

  Émis régulièrement par les points d'accès lors des trames de balisage (beacon frame).

  N'offre aucune sécurité même si certains points d'accès permettent la non émission de ces trames.

  Le SSID est émis lors de trame d'association.

L'authentification par le SSID

- Si vous ne faites que définir un SSID :

  on peut se connecter sur votre réseau sans vraiment le chercher, par hasard.

  Windows XP détecte les réseaux présents et peut se connecter automatiquement et si vous avez mis un DHCP en œuvre, on récupère une @ IP légale.

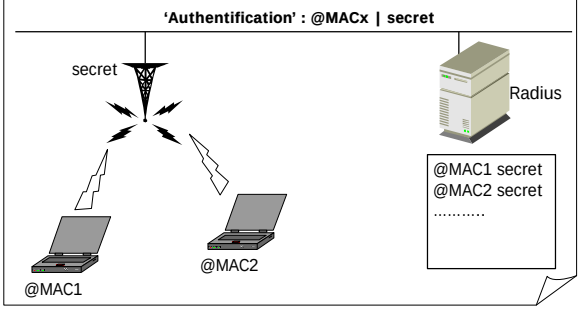
Filtrage des adresses MAC

- N'autoriser que certaines adresses à se connecter aux points d'accès.
- 2 méthodes :
  - Renseigner les @ MAC autorisées en local sur chaque point d'accès.
  - En utilisant un serveur Radius (serveur d'authentification pour centraliser les @ MAC autorisées).

Filtrage des adresses MAC

- Administration difficile en local surtout si le nombre de clients et de points d'accès sont importants.
- En centralisé, toutes les @MAC en clair dans le fichier de configuration radius.
- Le filtrage des @MAC est facilement contournable par substitution de l'@MAC. Il est possible d'usurper l'@MAC de la carte de quelqu'un d'autre

Centralisation des @MAC autorisées sur un serveur radius



Utiliser la sécurité de base des bornes

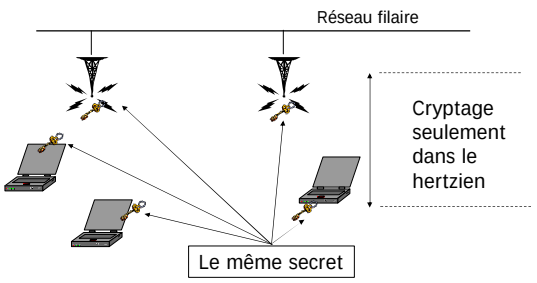
- Désactiver les fonctions non utilisées
  - ✓DHCP, Interface Web, SNMP, TFTP,
  - ✓Diffusion du SSID,
- Mettre des mots de passe de qualité et du filtrage @MAC pour tous les services utilisés (WEB, TELNET, SNMP, …)
- Installer le filtrage @MAC
- Mettre à jour le firmware des bornes et des cartes
- Régler la puissance des bornes au plus juste pour éviter les "débordements"

Wired Equivalent Privacy

- Objectif :
  Offrir une solution de cryptage des données.
- Principe :
  Chiffre le corps de la trame MAC et le CRC avec RC4 (algorithme de cryptage) en utilisant des clefs de 64 ou 128 bits.

  Le chiffrement n'est utilisé qu'entre les éléments 802.11. Il ne s'applique plus sur le réseau filaire.

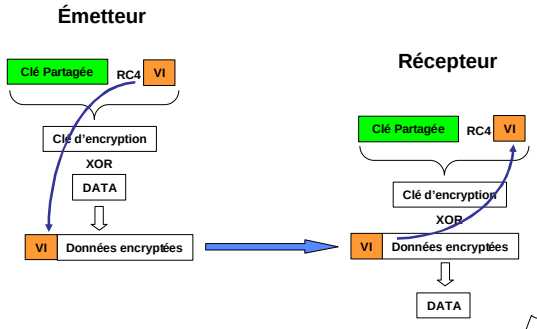
Wired Equivalent Privacy



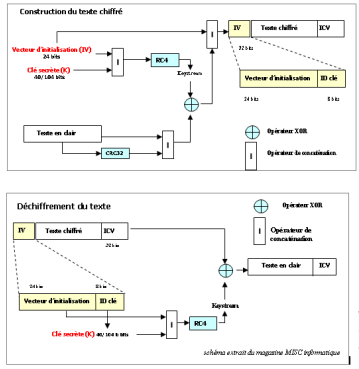
WEP – les points faibles

- Clés statiques partagées (40 bits "64", 104 bits "128")
  - Rarement changées
  - Vol de machine => vol de clef
  - Les autres qui partagent la clef peuvent lire vos trames
  - Possède une durée de vie longue
  - Diffusion d'une nouvelle clé difficile si le parc de mobile est important.
- Possibilité de choisir la clé dans l'espace des caractères imprimables.
  - Avec une clé de 40 bits et un jeu de 70 caractères : ~ 1.500 millions de combinaisons différentes. => Attaque par force brute possible.

WEP : Principe



WEP : principe détaillé



Texte chiffré = (texte en clair | ICV) *XOR* RC4 ((IV | K))

|| : Opérateur de concaténation,

ICV : Integrity Check Value (*Cyclic Redundancy Code* sur 32 bits)

IV: vecteur d'initialisation sur 24 bits

K : clé secrète partagée par l'AP et les clients (40 ou 104 bits)

Key-stream RC4 (IV | K): résultat de l'algorithme RC4 initialisé par IV et K

WEP offre une sécurité illusoire :
- Possibilité de découvrir la clé par des attaques

WEP – les points faibles

- Vecteur d'Initialisation (VI):
  - Choix du VI par compteur, nombre pseudo-aléatoire.
  - Par construction, on peut retomber fréquemment sur le même .
- Le trafic IP et ARP contient 0xAA comme 1er byte sur la trame en clair.
  - Connaissance d'un octet en clair et de l'octet équivalent en crypté → on en déduit le début du flux RC4.
- Existence de clés faibles avec RC4.

➔ **Attaque par cryptanalyse statistique.**

Conclusion sur la sécurité de base

- L'ensemble des fonctionnalités de base offertes par le 802.11 n'offre aucune sécurité digne de ce nom.
- **SSID** : c'est un nom de réseau.
- **Filtrage des @MAC** : on capture une @MAC.
- **WEP** : on utilise un logiciel pour casser la clé
  - Airsnort et Wepcrack

→Même sans connaissance approfondie de RC4 et du WEP, on peut casser votre cryptage WEP. Avec 500 Mo de données il suffit de quelques secondes de calcul pour déchiffrer la clef

Amélioration des fonctionnalités du 802.11

- Le 802.1x - EAP
- Le 802.11i

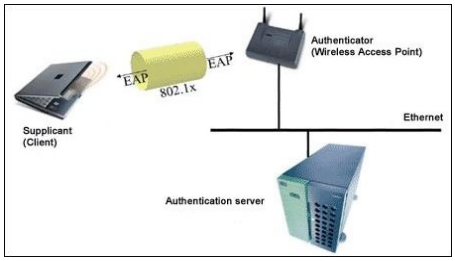
La sécurité avec le 802.1x

- Pour palier aux lacunes de sécurité du 802.11, l'IEEE propose **802.1x** qui est une architecture basée sur **EAP** (*Extensible Authentication Protocol)*.
- **EAP** a été choisi pour sa flexibilité et sa robustesse étant donné que ce dernier a fait ses preuves du fait de son implémentation comme solution d'authentification réseau de base dans de nombreuses architectures.

La norme IEEE 802.1x

- But :
  - Proposer un système d'authentification sécurisée
  - Proposer une solution de gestion dynamique des clés
- Moyens à mettre en œuvre :
  - Serveur d'authentification (type Radius)
  - Point d'accès supportant 802.1x
  - Client spécial sur le poste à authentifier
- Protocoles existants :
  - LEAP, EAP-TLS, EAP-TTLS, EAP-MD5, PEAP ...
    - Utilisation de mots de passe, certificats ...

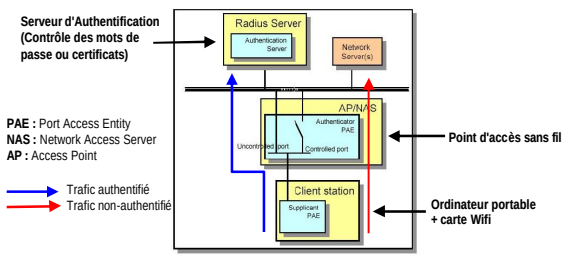
802.1x: Architecture et Nomenclature



Les trois différents rôles dans le IEEE 802.1X: Supplicant, Authenticator et Authentication Server (AAA Server: EAP Server, généralement RADIUS).

802.1x: Le Dual-port

- Principe



802.1x : Les protocoles d'authentification

- LEAP (Lightweight Authentication Protocol)
  - Développé par Cisco, utilisation de mot de passe
- PEAP (Protected)
  - Implémenté nativement dans Windows XP, utilise un certificat côté serveur et un mot de passe pour le client (authentification mutuelle)
- EAP-TLS (Transport Layer Security)
  - Implémenté également dans Windows XP, certificats pour serveur et client
- EAP-TTLS (Tunneled TLS)
  - Similaire à PEAP

802.1x : Déploiement sécurisé

- Problématique
  - Gérer l'hétérogénéité des plate-formes
    - PC, Mac ...
    - Windows, MacOS, Linux, FreeBSD ...
    - Type de carte Wifi (Aironet, ...)
  - Assurer l'authentification des utilisateurs
    - Mots de passe
    - Certificats
    - Adresse Mac
  - Sécuriser les échanges de données
    - Chiffrement

802.1x : Les solutions actuelles

- Cisco
  - Serveur Radius (ACS) , cartes et bornes d'accès Aironet (ACU, LEAP)

- Avantages :
  - Solution “clef en main”
  - Bon support technique
  - Fiabilité
- Inconvénients :
  - LEAP incompatible avec les autres cartes (donc ne répond pas au problème de l'hétérogénéité des plate-formes)
  - Solution payante
  - LEAP vulnérable aux attaques type “ Dictionnaire ”

802.1x : Les solutions actuelles

- MeetingHouse
  - Serveur Radius (Aegis)
  - Client EAP-TLS, PEAP, EAP-MD5, LEAP, EAP-TTLS pour toutes les plate-formes
  - Avantages :
    - Grande diversité des protocoles supportés
    - Interface simple et bon support technique
    - Déja déployé à grande échelle dans des universités américaines
    - Permet d'utiliser LEAP avec des cartes non-Cisco
  - Inconvénients :
    - Solution payante

802.1x : Les solutions actuelles

- Open Source
  - Freeradius
  - Xsupplicant (client d'authentification pour Linux)
  - Avantages :
    - Gratuit
    - Support et évolution assurés par une grande communauté d'utilisateurs
  - Inconvénients :
    - Encore en phase de développement
- Remarque :
  - Windows XP intègre 802.1x nativement

Conclusion sur 802.1x

- 802.1x propose un meilleur niveau de sécurité mais :
  - Des problèmes d'incompatibilité matérielle et logicielle.
  - Complexité de la configuration des postes clients
  - La gestion des mots de passe et des certificats peut être fastidieuse
  - Mise en œuvre difficile en environnement hétérogène.
  - Il faut faire évoluer le WEP => Wifi Protected Access (WPA)

Le groupe de travail IEEE 802.11i

Il définit deux niveaux :

- une solution de transition compatible avec le matériel existant, qui propose un nouveau protocole de gestion des clefs, TKIP (*Temporal Key Integrity Protocol*), qui génère et distribue des clefs WEP dynamiques, et qui sera inclus dans la certification WiFi de la WECA,
- une solution finale incompatible avec le matériel existant où 802.1X est obligatoire, avec l'algorithme de chiffrement RC4 remplacé par AES.

En cours de normalisation…

WPA = 802.11x + TKIP

- **Supporté par Windows XP (oct 2003)**
- **Temporal Key Integrity Protocol**
  - Vecteur d'Initialisation de 48 bits (x2 puissant)
  - Réinitialisation à l'établissement de la clef de session
  - Il délivre une clé par trame avec la clé de session
  - Remplace le CRC par une somme de contrôle cryptographique (MIC : *Message Integrity Code*) sur toute la trame, y compris les en-têtes : ceci rend caduques les attaques actuelles avec des trames 802.11b falsifiées.
- **Remplacement des points d'accès, cartes réseaux et programmes clients sans fil peut être nécessaire.**

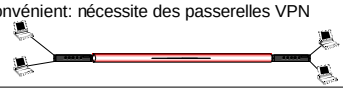
VPN : Les réseaux privés virtuels

- **Solution souvent adoptée par les opérateurs des hot-spots : les WISP**
- Rôle des VPNs (Virtual Private Network) : fournir un tunnel sécurisé de bout en bout entre un client et un serveur.
- **Pourquoi utiliser VPN ?**
  - 802.1x est très récent.
  - L'infrastructure VPN est indépendante du réseau sans fil et la facturation est simplifiée
  - VPN offre toutes les fonctions que l'on recherche:
    - Authentification et autorisation d'accès
      - Authentification des deux extrémités
    - Chiffrage (confidentialité) et protection (intégrité) des données
      - Chiffrage des adresses sources et destination (avec IPSec)

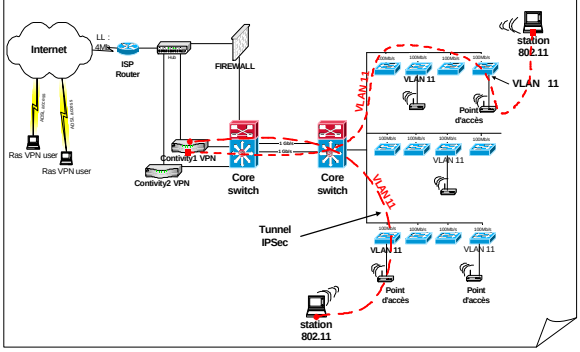
IPSec appliqué aux VPN

- **IPSec mode transport:** En mode transport, la session IPSec est établie entre deux hôtes
  - Avantage : la session est sécurisée de bout en bout
  - Inconvénient : nécessité d'une implémentation de IPSec sur tous les hosts; autant de sessions IPSec que de couples de hosts

- **IPSec mode tunnel:** En mode tunnel, la session IPSec est établie entre deux passerelles IPSec, ou un host et une passerelle
  - Avantage: l'ensemble des communications traversant les passerelles VPN peuvent être sécurisées; pas de modification des hosts
  - Inconvénient: nécessite des passerelles VPN



Sécurisation VPN/IPSec : cas réel



Impact d'IPSec en terme de performance

- Le rapport « charge totale/ charge utile » augmente.

Paquet d'origine		**Header IP**	**TCP**	**DATA**
Mode Tunnel	**Nouveau header IP**	**IPSec**	**Header IP**	**TCP**	**DATA**

- Coût en terme de temps supplémentaire engendré par tous les calculs que nécessite
  - MD5 (hachage pour l'intégrité)
  - 3DES (algorithme symétrique pour confidentialité)
  - RSA (authentification par signature à clé publique)

IPSec – VPN : Conclusion

- **IPsec** est à ce jour le protocole le plus utilisé dans les VPNs.
- Standard de référence, IPsec s'appuie sur différents protocoles et algorithmes en fonction du niveau de sécurité souhaité :
  - **Authentification** par signature électronique à clé publique (RSA).
  - **Contrôle de l'intégrité** par fonction de hachage (MD5).
  - **Confidentialité** par l'intermédiaire d'algorithmes symétriques, tels que DES, 3DES ou IDEA.
- Aujourd'hui, l'utilisation d'un VPN est la manière la plus fiable de sécuriser un réseau wireless.

  C'est aussi la méthode la plus utilisée *lorsqu'il y a volonté de sécurisation*.
- Mais il faut savoir que les performances vont diminuer (significativement) : Bande passante diminuée de 30% en moyenne.

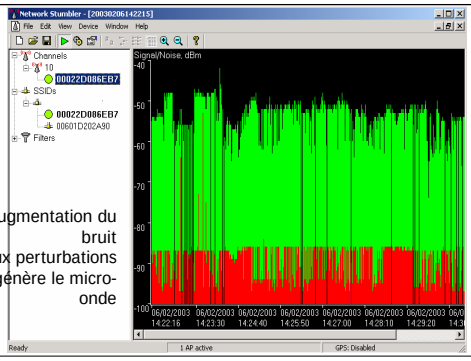
Architecturer correctement ses WLAN

- Les réseaux sans fil peuvent être considérés comme extérieurs au périmètre sous contrôle (de confiance), donc comme les flux Internet.
- Il faut segmenter les réseaux sans fil sur des DMZ (zones démilitarisées), derrière des passerelles de sécurité, avec un filtrage et une journalisation avant d'accéder au réseau privé.
- Cette sécurité est complémentaire à l'authentification et au contrôle d'accès sur l'interface « *air* » réalisée par la borne.

Outils de détection sous Windows

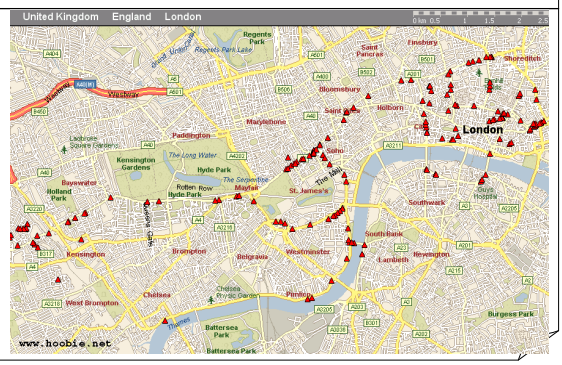
- Netstumbler (http://www.netstumbler.com)
  - Fournit peu d'information.
  - Interface conviviale.
  - Historique ratio signal/bruit.
  - Fonctionne avec différentes cartes (Cisco, Orinoco, Netgear, …).
- Netstumbler pour Ipaq
  - Plus petit et plus discret

Outils de détection : Netstumbler



Augmentation du bruit dû aux perturbations que génère le micro-onde

"Wireless Map" obtenue avec Netstumbler



Nécessité d'audit et de surveillance

- En plus des trames de données et de contrôle, beaucoup de trames d'administration circulent sur le réseau;
- L'audit permet de détecter
  - les réseaux sauvages,
  - les stations mal ou auto-configurées

  et d'évaluer la sécurité des réseaux sans fil
- La surveillance permet de détecter
  - les intrusions,
  - les écoutes,
  - Les fausses bornes.

Outils de détection sous Linux

- Kismet (outil d'audit)
  - ✓Données en temps réel
  - ✓Signal de réception pour géolocalisation
  - ✓Sauvegarde du trafic pour étude plus poussée
  - ✓Affichage du type de client
  - ✓Découverte de SSID
- Détection d'anomalies et de pièges à *Wardrive*

Outils de détection sous Linux

- AirTraf (http://airtraf.sourceforge.net)
  - Affichage en temps réel
    - Bande passante utilisée
    - Liste des clients détectés
    - Possibilité de faire des statistiques (via base MySQL)
- WifiScanner (http://wifiscanner.sourceforge.net)
  - Détection et affichage de l'architecture réseau
  - Trafic entièrement sauvegardé
    - Pour l'analyse hors ligne
  - Analyse de plus de 99% des trames réseaux
  - Module d'analyse et de détection d'anomalies
    - Surveillance passive d'un réseau
  - Discret et quasiment indétectable
    - Pas de paquets radio envoyés

Types d'informations récupérées

Trois sortes de paquets 802.11b:

- Paquets d'administration
  - Beacon frame, Probe request/response
    - Facile à détecter
      - 10 paquets par seconde
      - Portée importante
    - Envoyés par point d'accès ou client en mode ad-hoc
    - Ces paquets contiennent:
      - SSID
      - Horodatage
      - Caractéristiques systèmes
  - Association
    - Envoyé en début de connexion
  - Authentification
    - Envoyé lors de l'établissement du protocole de dialogue

Types d'informations récupérées

- Trames de contrôles
  - Trafic actif et existant
  - Permet de détecter des équipements en aveugle
- Trames de données
  - Identification
  - Mot de passe
  - Courrier électronique
  - Informations ARP
  - Weak IV (cassage du Wep)
  - Trames broadcast venant du réseau filaire

Conclusion : Préconisation minimum

- Points d'accès
  - Placer les points d'accès le plus loin possible des murs et fenêtres donnant sur l'extérieur et régler la puissance d'émission.
  - Analyser régulièrement les zones sensibles avec un portable pour découvrir d'éventuels points d'accès «sauvages».
- SSID
  - Supprimer l'émission de broadcast des trames de balisage (beacon frame).

Conclusion : Préconisation minimum

- Filtrer les @MAC
- Mettre en œuvre le WEP
- Administration
  - Modifier les passwords SNMP.
  - Interdire l'accès à l'administration par le WLAN.

Conclusion : Sécuriser son WLAN

- **On peut utiliser 802.1x.**
  Si le parc des éléments 802.11b est récent et homogène.
  - EAP/TLS : Nécessite des certificats pour chaque client.
  - EAP/TTLS : Authentification du client par login/password

  Attention, des failles ont déjà été trouvées dans 802.1x
  http://www.cs.umd.edu/~waa/1x.pdf
- **Ou attendre la maturité de WPA.**
- **Ou utiliser VPN avec IPSec**.
  Si le parc est hétérogène. C'est la solution la plus utilisée lorsque le WLAN est sécurisé.

IS95

IS95

- Interim Standard 95 : 2ème génération sans-fil aux États-unis avec IS136
- IS136 : Multiplexage TDMA, concurrent du GSM
- IS95 : Technique CDMA (société Qualcomm)
  - concurrent du GSM
  - utilise 2 bandes de fréquences 800 MHz (cohabite avec AMPS analogique sur une largeur de 25 MHz) et 1900MHz
  - fonctionne en séquence directe, et une communication occupe 1,25 MHz dans chaque sens (forward direction =descendant, reverse direction = montant)
  - utilise le soft-handoff ou soft-handover

IS95

- Architecture quasiment identique au GSM, sauf :
  - pas de BSC, les MSC sont reliés aux BS.
  - synchronisation par un système GPS
- Interface radio :
  - Étalement -> [Chips] -> Modulation de phase

IS95

- étalement
  - codes orthogonaux : résultat nul pour le produit scalaire entre 2 codes.
    Exemple : matrices de Walsh-Hadamard
  - séquences pseudo-aléatoires : corrélation croisée quasi nulle, auto-corrélation = longueur du code
  - Exemple:
    - S_1=(11111000110111010100000100101100)
    - S_2=(11111000110111010100000100101100)
    - ➢ $S_1 \otimes S_2$=15 $S_1 \otimes S_1$=31

IS95

- Matrices de Walsh-Hadamard
- Motif W_1=[0], L multiples de 2
- $W_L = \begin{bmatrix} W_{L/2} & W_{L/2} \\ W_{L/2} & \overline{W_{L/2}} \end{bmatrix}$
- Exemples

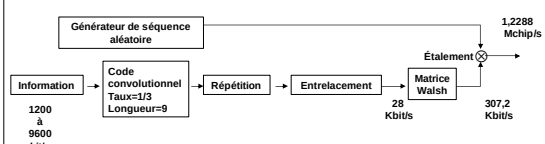
W_1=[0], $W_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, $W_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$

Ex. les lignes 3 et 4 sont orthogonales entre elles.

Ces codes peuvent jouer un rôle de code correcteur.

IS95 - Sens montant

- pour chaque canal physique, l'IS95 génère une séquence aléatoire (long mask) qui module et multiplexe l'information utile par étalement (CDMA)
- le générateur est constitué d'un registre à décalage à 42 cases (période de 2^{42}-1) → long pour un débit de 1,2288 MChip/s. Période de 41 jours entre 2 codes identiques.



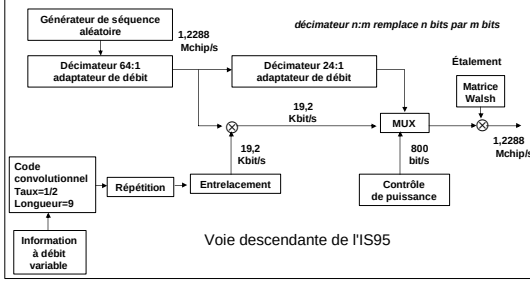
Voie montante de l'IS95

IS95 - Sens montant

- 4 débits utilisateur de 1200, 2400, 4800 et 9600 bit/s sont protégés par un code convolutionnel. Les données sont répétées (jusqu'à 8 fois pour le plus faible débit) pour obtenir un débit régulier de 9600 bit/s.
- La protection (1/3) nécessite un débit de 3x9600=28800bit/s.
- La matrice de Walsh-Hadamard de dimension 64 assure une autre protection C(64,6). Chaque bloc de 6 bits est codé sur 64 bits, ce qui donne un débit de 307,2 Kbit/s
- L'étalement est la dernière phase de la modulation binaire. Chaque bit est étalé par 4 chips.
  Le débit en sortie est donc de 1,2288 MChip/s et est envoyé au modulateur QPSK (Modulation de phase en quadrature) pour émission.

IS95 - Sens descendant

- protection contre les erreurs moins performante (transmission par un seul émetteur, la BS), meilleur contrôle, synchronisation parfaite
- contrôle de puissance d'émission des utilisateurs (800bit/s)



Voie descendante de l'IS95

IS95 - Sens descendant

- Les décimateurs abaissent le débit de la séquence aléatoire pour le rendre compatible au débit d'information.
- Le débit en sortie est donc de 1,2288 MChip/s et est envoyé au modulateur QPSK (Modulation de phase en quadrature) pour émission.

IS95 – Canaux logiques

- Un canal physique : une porteuse ET un code
- Les canaux logiques gèrent l'information dans les canaux suivants :

Canal logique	Sens de la transmission	Dédié ou commun
Pilot	Descendant	Commun
Sync	Descendant	Commun
Paging	Descendant	Commun
Access	Montant	Commun
Traffic - Trafic	Duplex	Dédié
Traffic - Signalisation	Duplex	Dédié
Traffic – Contrôle de puissance	Descendant	Dédié

IS95 – Canaux logiques

- Le terminal choisit la BS (écoute du canal *Pilot*), se synchronise (canal *Sync*), scrute les infos du canal *Paging* pour accéder au système. Il est alors enregistré.
- Lors d'un appel, il sollicite le canal *Access*, la BS lui répond par le canal *Paging* et obtient éventuellement un canal *Traffic.*

IS95 – Canaux logiques

- Canal Pilot
  - Une BS envoie une série de zéros sur la porteuse principale de la cellule sans modulation mais avec des décalages (PN_offset) de 64 bits pour éviter les confusions entre BS.
  - Utilise le GPS (Global Positionning System) pour la synchronisation.
  - $Walsh_0$ (1ère ligne)
- Canal Sync
  - Canal à 1200 bit/s, code convolutionnel ½, répétition, entrelacement puis $Walsh_{32}$ (33ème ligne)
  - Diffuse le n° de l'identificateur du sous-réseau, le décalage de la cellule (PN_offset), le débit du canal de Paging, etc.

IS95 – Canaux logiques

- Canal Paging
  - Ressource commune diffusant le nombre de canaux de paging, paramètres de l'accès aléatoire, liste des BS voisines, liste de fréquences disponibles, localisation, messages d'acquittement, etc.
  - lignes 1 à 7 de Walsh (1 à 7 canaux, nombre diffusé sur le 1er canal)
  - débit de 4800 ou 9600 bit/s
- Canal Access
  - utilisé pour transmettre vers la BS
  - jusqu'à 32 canaux Access au débit de 4800 bit/s
  - accès aléatoire "Slotted Aloha"
  - le terminal dépose une requête attend un acquittement sinon réitère sa demande (jusqu'à un nombre maxi - sonde ="probe") puis recommence avec un niveau de puissance supérieur

IS95 – Canaux logiques

- Canal Traffic
  - sert pour l'information ou la signalisation dédiée
  - débit de 1200, 2400, 4800 ou 9600 bit/s soit 24, 48, 96 ou 192 bit par trame de 20 ms.
  - Code CRC
  - Les trames contiennent soit de l'information, soit de la signalisation (pendant les silences) soit un mélange des 2
- Sur la voie montante, jusqu'à 62 canaux de trafic, identifiés par le numéro de série des terminaux ou ESN (Electronic Serial Number)

IS95 - Soft-Handover

- Utilisé dans le système IS95 pour la 1ère fois.
- A l'intersection de cellules le lien est établi avec plusieurs cellules (6 max). La synchronisation des signaux est assurée par GPS.
- Pendant le déroulement du handover : 4 listes :
  - cellules actives
  - candidates
  - voisines
  - restantes.
- Utilise un mécanisme de double seuil sur la puissance plus un de temporisation

IS41

- La 1ère génération de téléphonie cellulaire a normalisé l'interface radio, mais les parties fixes se sont développées de multiples manières.
- Pas de solution simple pour passer d'un réseau à un autre
- Suite au développement du GSM, les américains ont créé le standard IS41 avec une architecture (et un vocabulaire) très proche du GSM (MSC, HLR, VLR)

CDMA2000

CDMA2000

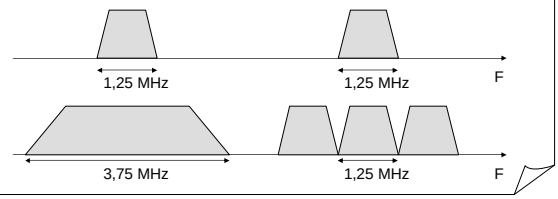
- Né lors d'une conférence internationale de l'UIT en 1992
- Programme IMT2000 (International Mobile Telecommunications System)
- Bande de fréquences de 2 GHz rendue disponible
- Proposition de CDMA2000 (suite de l'IS95 -CDMA-) et UWC136 (suite de l'IS136 -TDMA- concurrent de l'IS95 qui passe en GPRS et EDGE pour augmenter le débit)
- En Europe et Japon, W-CDMA (CDMA large bande) associé au TD-CDMA pour former l'UMTS.

CDMA2000

- Signalisation de la partie filaire régie par le protocole IS41.
- Des accords de compatibilité avec le protocole MAP de l'UMTS (repris du GSM) sont envisagés.
- La bande de fréquences attribuée est déjà occupée (!!!) et seules des bandes de 10MHz sont libres. Les autres devront être libérées en cas de succès commercial. Pour l'UMTS, les bandes attribuées sont "nouvelles"
- CDMA2000 doit fonctionner quelque soit la taille de cellule, pour piéton, véhicule et en Boucle Locale Radio.

CDMA2000

- CDMA2000 doit co-exister avec IS95. L'étalement prévu est 3 fois supérieur. Pour rester compatible, l'information est découpée en 3 parties qui s'étalent séparément sur 3 bandes étroites. En cas de non sollicitation IS95, la voie montante reste large bande



CDMA2000

- Flexibilité multiporteuse :
  - possibilité d'utiliser 2 ou 3 porteuses adjacentes pour un même signal (qui est alors reconstruit à partir des 2 ou 3 signaux)
  - débit de 1,2288 Mchip/s pour chaque partie.

CDMA2000 - Architecture

- 3 plans ayant chacun 7 couches : Plan mode circuit, plan mode paquet, plan de signalisation
  - Couches hautes 3 à 7
  - Couche liaison
  - Couche physique

CDMA2000 - couches hautes

- Le **plan circuit** met en service et garantit une communication
- Le **plan paquet** assure l'acheminement des flux paquet par paquet depuis ou vers un mobile. Il les rend compatibles avec les autres réseaux (TCP/IP par exemple) Il fournit un service de SMS
- Le **plan de signalisation** contrôle le fonctionnement du mobile

CDMA2000 - couche liaison

- 2 sous-couches :
  - LAC = Link Access Control
  - MAC = Media Access Control

Dans les couches supérieures, les performances de la couche physique ne sont pas connues.

Lors d'une requête, la couche 2 est traversée et la couche MAC multiplexe l'information hétérogène sur un canal physique.

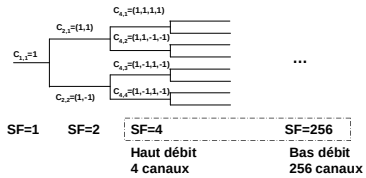
- PLICF = Physical Layer Independant Convergence Function
- PLDCF = Physical Layer Dependant Convergence Function
  - Instance-Specific PLDCF
  - PLDCF MUX et QoS

CDMA2000 - couche liaison

- La couche PLICF comporte de nombreux canaux logiques (**f**orward/**r**everse, **c**ommun ou **d**édié, fonction)
  Trafic Channel : f/r-dtch, f/r-ctch
  MAC Channel : f/r-dmch_control, r-cmch_control, f-cmch_control
  Signaling Channel : dsch, csch
- La couche PLDCF transforme les canaux logiques de la couche PLICF en canaux physiques conformes) la couche de transmission utilisée.
  Elle gère la QoS des flux de données en fonction de 2 priorités : le délai de livraison, le débit de la liaison
  Utilise les méthodes de retransmission ARQ (Automatic Repeat reQuest) en cas d'erreur.

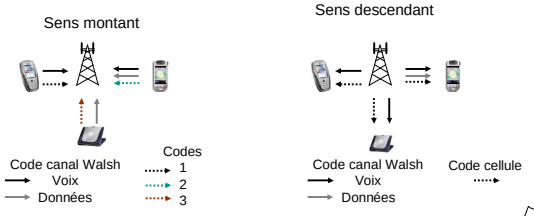
CDMA2000 - couche physique

- canal physique = combinaison d'un code canal et d'une séquence aléatoire
- possibilité d'utiliser un Spreading Factor de 4 à 256
- possibilité de multiplexer des codes à débit variable 2 de SF=4 et 128 de SF=256



CDMA2000 - couche physique

- Sens montant : chaque utilisateur a sa propre séquence pseudo-aléatoire
- Sens descendant : une seule séquence est allouée (code cellule)



CDMA2000 - canaux physiques

F-PICH	Forward Pilot CHannel	Descendant
F-TDPICH	Forward Transmit Diversity Pilot CHannel	
F-PCH	Forward Paging CHannel	
F-SYNC	Forward SYNC CHannel	
F-CCCH	Forward Common Control CHannel	
F-BCCH	Forward Broadcast Control CHannel	
F-QPCH	Forward Quick Paging CHannel	
F-CACH	Forward Channel Assignment CHannel	
F-CPCCH	Forward Common Power Control CHannel	
R-ACH	Reverse Access CHannel	Montant
R-CCCH	Reverse Common Control CHannel	
R-EACH	Reverse Enhanced Access CHannel	

CDMA2000 - canaux physiques

- F-PICH (Pilot)
  - Permet de sélectionner la "meilleure" station de base.
  - Synchronisation identique à IS95 (PN_Offset)
  - Si plusieurs antennes pour une BS, plusieurs pilotes : F-TDPICH est alors nécessaire
- Le mobile se synchronise sur F-SYNC avec la base et utilise le canal F-BCCH pour récupérer les informations nécessaires et est ensuite en état "idle".
- Le mobile peut capter un appel grâce au Paging ou être à l'origine d'un appel. R-ACH sert à répondre au Paging ou à initier un appel

CDMA2000 - canaux physiques

- Service paquet : un utilisateur s'attache à un point d'accès et écoute (pas de réservation). Un slot transporte un F-QPCH pour l'informer de l'arrivée d'un paquet. Le terminal reçoit alors le message dans le F-CCCH
- Dans le sens montant, pour envoyer un message :
  - soit avec le canal R-EACH (accès aléatoire)
  - soit requête au R-ACH puis réponse par le F-CACH et envoi par le R-CCCH (utilisé par le seul utilisateur qui en a fait la demande – pas de collision)

CDMA2000 - canaux physiques

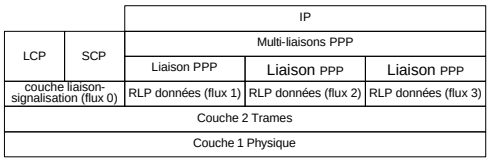
- D'autres canaux dédiés existent, par exemple :
  - F-FCH = Forward Fundamental Channel peut être attribué à un terminal. Pour des débits supérieurs, d'autres canaux F-SCH1, F-SCH2 (Supplement) peuvent être affectés
- A la demande d'un canal dédié, le terminal et le réseau négocient dans une procédure appelée "configuration de service" où sont définis le facteur d'étalement, le débit, la taille des trame, le type de code correcteur… pour la voie montante et descendante avec des numéros de configuration prédéfinis.

CDMA2000 - HDR

- High Data Rate : proposition de la société Qualcomm pour mettre en place un service IP sur la couche physique de CDMA2000. Le protocole IP à la fonction d'un réseau fédérateur ou de transport. Le CDMA2000 devient un réseau d'accès au transport IP.
- La complexité de gestion des différents canaux fait baisser le débit. Pour cela l'accès TDMA est introduit où tous les utilisateurs sont multiplexés dans le temps avec des intervalles modulables et les hauts débits sont envoyés dans les fréquences les plus élevées.

CDMA2000 - HDR

- Le protocole PPP (Point-to-Point Protocol) a été choisi pour s'intercaler entre CDMA2000 et IP
- 2 protocoles LCP (Link Control Protocol) et SCP (Stream Control Protocol) instruisent la signalisation
  LCP négocie l'octroi d'une liaison radio avec tous les paramètres nécessaires. SCP contrôle la retransmission des segments perdus.
- RLP (Radio Link Protocol) se situe juste en dessous.



CDMA2000 - Réseau d'accès

- L'adresse IP d'un utilisateur est modifiée par le protocole IP Mobile.
- L'obtention et la résolution de l'adresse IP sont réalisées par des serveurs DHCP et DNS.
- Un serveur RADIUS sécurise les liaisons PPP.
- L'ensemble est régi par 2 protocoles SNMP (Simple Network Management Protocol) pour la gestion et HTTPS (HyperText Transfer Protocole Secure) pour la sécurité.
- CDMA a l'avantage de liaisons flexibles (multiporteuses, QoS adaptées à la demande et une interconnexion aisée avec IP
- HDR est une solution pour faire converger CDMA2000 et IP.

Services 2G et 3G

Support basé sur G. Pujolle

Services 2G

- Depuis les SMS (Short Message Service) ... jusqu'aux portails mobiles WAP (Wireless Application Protocol)
- Cible :
  - Grand public
  - Professionnels : commerciaux, agents de maintenance, visiteurs médicaux, livreurs…

Services Internet mobiles

- terminal = système d'exploitation réduit + micro-navigateur : téléphone, PDA…
- services WAP, i-mode, HTML léger, jeux, télévision interactive, VoxML, VoiceXML : tout se passe sur le serveur = aucune persistance de l'information sur le terminal
- Exemples : messagerie électronique, internet, intranet, base de données, serveur LDAP (Lightweight Directory Access Protocol), ERP (Enterprise Resource Planning)…

Services Internet mobiles

- Services multiaccès
  - pour téléphones équipés de micro-navigateurs
  - langage WML (Wireless Markup Language) très grandes contraintes
  - Évolution : (HTML utilisation de langages dérivés du HTML:
    xHTML (eXtensive HTML), Tiny HTML (allégé) C-HTML (Compact)
- Services à base de *push*
  - SMS et EMS (Enhanced Messaging Service) envoyés par une application 2G

Portails mobiles

- Apparition d'interface conviviale professionnelle de type Web pour rassembler, distiller les informations :
  - portail B-to-E (*Business-to-employees*)
  - portail B-to-B (*Business-to-business*)
  - portail B-to-C (*Business-to-consumers*)
- Accès aux données, e-mail, alertes par SMS, etc.

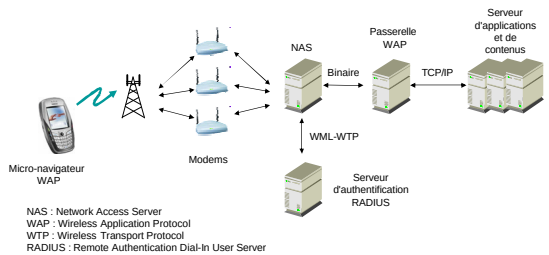
M-commerce et services grand public

- Contrairement aux services de l'Internet fixe, les services mobiles sont payants
- et l'utilisateur est identifié lors de la connexion : intérêt pour la facturation, mais aussi pour la publicité ciblée (Cell Broadcast)
- Les applications ne doivent pas se contenter de copier les applications Web classiques (échec du WAP)
- Ajout de services paiement carte bleue, géolocalisation, etc.

Wap

- Utilise un langage dérivé du XML, le WML et un langage de script WMLScript.
- Contenus sous forme de mini-pages ou cards regroupées en decks

WAP : architecture



I-Mode (NTT DoCoMo) est à base de HTML et n'utilise pas de passerelle de conversion en binaire

SMS (Short Message Service)

- Échange de message à l'initiative d'un opérateur, d'une entreprise ou d'un particulier (push) ou à celle du propriétaire (mode pull)
- Loisirs : sonneries, logos, configuration à distance (OTA = Over The Air)
- Commerce mobile : jusqu'à 3 flux SMS pour une transaction
- Service d'information (résultats sportifs, météo, etc.)
- Service d'entreprise

SMS

- L'émission d'un SMS passe par un SMSC (Short Message Service Center) qui fonctionne en store-and-forward et conserve les messages jusqu'à transmission au destinataire.

  Le SMSC reçoit les messages des modems, autres SMSC, internet, etc.
- Opérateurs de SMS : passent un accord avec un opérateur de réseau numérique pour l'accès à leur SMSC.

Applications avancées

- Push OTA = envoi de messages texte ou binaire pour effectuer des opérations à distance :
  - Paramétrage d'accès WAP
  - Mélodies et icônes
  - Contacts et agendas
- Évolutions multimédias du SMS :
  - EMS (Enhanced Messaging Service
  - MMS (Multimedia Messaging Service)
- SMS Cell Broadcast (SMS/CB)
  exemple : envoi de message dans une cellule à des abonnés (un canal par type d'information)
  93 caractères maxi * 15 = macromessage
  passe par un CBC (Cell Broadcast Center)

Services 3G

- Augmentation du débit (64 K, 384K à 2 Mbit/s en théorie)
- Augmentation de la puissance de calcul embarquée dans les terminaux
- Applications voix, multimédia, vidéo, données
- Normes du multimédia :
  - JPEG (Joint Photographic Expert Group)
  - MPEG (Moving Pictures …)
  - MHEG (Multimedia and Hypermedia …)
  - VRML (Virtual Reality Modeling Language)

Équipements terminaux multimédia

- Recommandations UIT-T

	Réseaux téléphoniques
Vidéo	H261 - H263
Audio	G723 - G729
Données	T120
Multiplex	H223
Contrôle	H245

Codage et compression

- Point clé pour l'intégration de la vidéo dans les communications mobiles
- Taux obtenus dans les normes actuelles :
  - images fixes : 10 à 50 (~20), JPEG, JPEG2000
  - vidéo : 50 à 200(~100)
- Exemple visioconférence : norme H.261 ou p*64 pour p fois 64 kbit/s de débit (max p=30)
- Format CIF (Common Intermediate Format) entre les 625 lignes 50Hz en Europe et 525 lignes 60Hz en Amérique du Nord et Japon
- et QCIF (Quarter CIF) avec 288 lignes à 30 Hz.

Codage et compression : MPEG

- MPEG et DVB de plus en plus utilisés dans les terminaux mobiles
  MPEG : 1,5 Mbit/s pour une qualité télévision (TV)
- MPEG-2 choisi pour la TV numérique, soutenu par le consortium DVB.
  - 3 types de trame :
    - I : codage Interne
    - P : codage Prédictif
    - B : codage prédictif Bidirectionnel

Codage et compression : MPEG-2

- I : codage Interne
  Pas de référence à d'autres trames,
  Compression basée sur la Transformée en Cosinus Discrète sur des blocs 8x8 pixels, lecture en zig-zag, quantification, codage différentiel et Huffmann
- P : codage Prédictif
  Ajout d'une compensation de mouvement (MC) par rapport aux trames (I et P) précédentes
- B : codage prédictif Bidirectionnel
  Ajout d'une compensation de mouvement (MC) par rapport aux trames (I et P) précédentes et suivantes
- Ces trames constituent des Group Of Pictures (GOP)

Exemple : I B B P B B P B B P B B I

Codage et compression : MPEG-2

- Codeur complexe -> cher
- Décodeur de prix abordable en grande série (hardware)
- Particularités :
  - Taille des trames variables
  - Importance des trames I lors de la transmission
- Services CBR (Constant Bit Rate) ou VBR (Variable Bit Rate)

Codage et compression : MPEG-2

- MPEG-2 : 3 couches
  - MPEG-2-1 : couche système, multiplexage du flux
  - MPEG-2-2 : compression vidéo
  - MPEG-2-3 : compression audio (MP3 est en fait du MPEG-2-3)

  + une signalisation sous formes de tables

Codage et compression : MPEG-4 et MPEG-7

- MPEG-4 est déjà présent dans les caméscopes numériques
- Codage basé sur la segmentation des images en objets pour un codage adapté : nécessité de reconnaître ces objets au préalable
- Hiérarchisation des flux avec des priorités
- MPEG-7 est basé sur une indexation des contenus, assure une compatibilité XML et vise une intégration sur le Web

Réseaux futurs 4G

Limites des systèmes 3G

- UMTS : bande passante limitée
- 4G :
  - augmentation du débit
  - unification des solutions mobiles avec un terminal unique
- 5G :
  - unification des interfaces radio
  - unification des techniques d'accès
  - unification des services

Générations de réseaux mobiles et sans fil

	1980	1990	2000	2010	2020
Génération	1G	2G	3G	4G	5G
Innovation	analogique	numérique	Paquet	Haut-débit IP Mobile	?
Réseau de mobiles	cellule analogique	cellule numérique GSM, IS95…	IMT2000 UMTS, W-CDMA, CDMA2000, Edge	Accès large bande par unification 3G	Accès large bande
Réseaux sans fil	sans fil analogique	sans fil numérique IEEE802.11b Bluetooth DECT <10Mbit/s	IEEE802.11a DECT <50Mbit/s	ITS, HAPS <100Mbit/s	ITS, HAPS <1Gbit/s

Technologie 4G

- Unification des solutions existantes
- Travaux IEEE802.15 : choix de Bluetooth 2.0 comme WPAN (Wireless Personal Area Network) ~10 Mbit/s sur une centaine de mètres
- Amélioration de la QoS : norme IEEE802.11e pour la téléphonie et la visioconférence
- Généralisation de l'environnement IP
- MAN : norme IEEE802.16 faible mobilité = débit ~100 Mbit/s

Satellites

- Utilisation des satellites géostationnaires :
  - cellules de diamètre 50 kms
  - fréquences entre 30 et 60 GHz
  - facteur de réutilisation de 20000 sur la terre
- Problèmes à résoudre :
  - maîtriser la propagation à ces fréquences
  - limiter la puissance d'émission et de réception
  - taille de l'antenne voisine de celle d'un GSM
  - ces fréquences ne rentrent pas dans les bâtiments

Terminaux 4G

- Terminal mobile et sans fil
- Réseau cœur = celui de UMTS, réseau IP, protocole IP Mobile
- Terminal communiquant avec les serveurs des opérateurs pour choisir le meilleur réseau
- Logiciel embarqué capable de choisir le meilleur
- Gestion des handovers hétérogènes

Équipement mobile

- Antennes intelligentes (Smart Antenna)
  capable de traiter les signaux reçus pour améliorer le flux destiné à l'utilisateur
- Radio logiciels (Software Radio)
  capable de redéfinir toutes les couches dynamiquement
  Utilisation de DSP (Digital Signal Processor) ou circuits de type ASIC (Application Specific Integrated Circuit) mais ils sont gourmands en énergie…

Applications 4G

- Images animées, vidéo à la demande, télévision, visioconférence
- MPEG12 : baisser le débit à 256 voire 128 ou 64 Kbit/s
- VHE (Virtual Home Environment) pour se connecter n'importe où, sur tout type de terminal et retrouver son environnement de travail personnel sécurisé
- Nomadisme
  Exemple : reprise d'une session de travail, même en cas de déconnexion)
- Internet ambiant, diffus… partout

Perspectives

- 5G : à inventer…
- HAPS (High Altitude Stratosphéric Platform) en complément des satellites géostationnaires :
  - ballons stratosphériques à haute altitude
  - avion de type AWACS à basse altitude
- 1ère bande de 600 MHz allouée dans la bande des 47-48 GHz

Bluetooth

d'après le cours de M. Guindon
Université de Sherbrooke

Plan

- Introduction
- Quelques exemples d'utilisations
- Point de vue technique
- Principle de fonctionnement
- Sécurité

D'où vient le nom 'Bluetooth' ?

Bluetooth est le nom d'un chef Viking du nord : *Harald Blaatand* ("Harald la dent bleue"). Celui-ci réussit l'exploit d'unifier au sein d'un même royaume le Danemark et la Norvège, à l'époque où l'Europe était divisée par des querelles de religions et de territoires.

Aujourd'hui Bluetooth mène une véritable croisade des temps modernes pour unifier l'ensemble des constructeurs et leurs appareils électroniques grâce à un nouveau standard de communication sans fil.

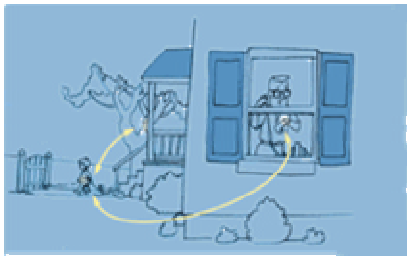
Quels produits incorporent cette technologie?

Où la technologie est disponible?

Usages

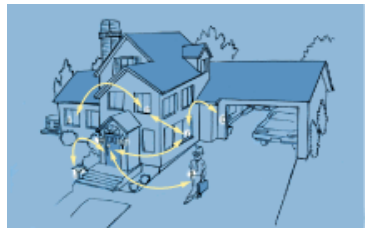
Contrôles : accès, lumière, températures...

Usages



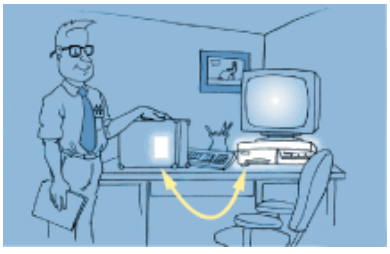
Détecteur de présence : intrusion, mais aussi évasion...

Usages



Commande à distance : porte, lumière, garage...

Usages



Synchronisation des informations...

Usages

Communication avec les équipements NTIC...

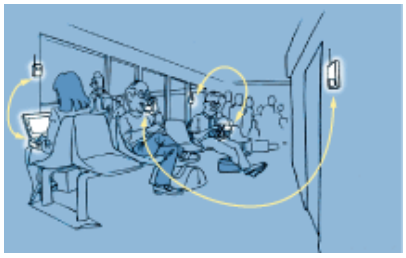
Usages

Téléchargement des GUI d'équipements variés...

Usages

Télépaiement...

Usages

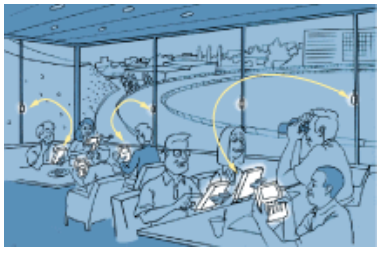


Accès Internet et autres réseaux...

Usages

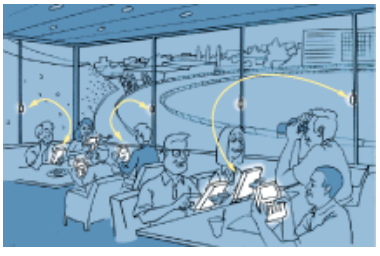
Echanges de cartes de visites...

Usages



Prises de commandes...

Usages



Prises de commandes...

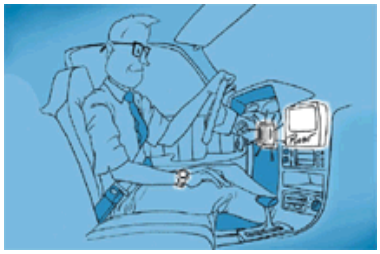
Usages

InfoFueling : Téléchargement dans le véhicule auprès de bornes...

Usages

Paramétrisation automatique : déverrouillage, le siège se règle à votre hauteur, la radio se met sur votre station préférée

Usages



Vous recevez un appel téléphonique pendant que vous conduisez, celui-ci est automatiquement transmis à votre autoradio (son sur les HP)

Le Bluetooth Special Interest Group (SIG)

Microsoft MOTOROLA NOKIA TOSHIBA

3com agere systems ERICSSON IBM intel

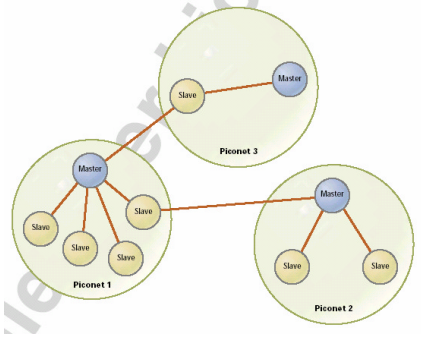
Comment Bluetooth Fonctionne?

- Élimine fil et câble entre les différents modules
- Facilite aussi bien les communications de données et de voix
- Permet de créer des réseaux ad hoc entre plusieurs modules Bluetooth

Comment Bluetooth Fonctionne?

- Puce à fréquence embarquée dans le module électronique
- Utilise la bande radio 2.4 -> 2.48 GHz pour communiquer
- Établissement de Piconets

Piconet & Scatternet



Source: PWC 2000 Technology Forecast

Piconet & Scatternet

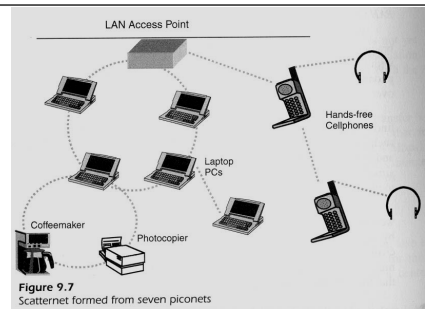
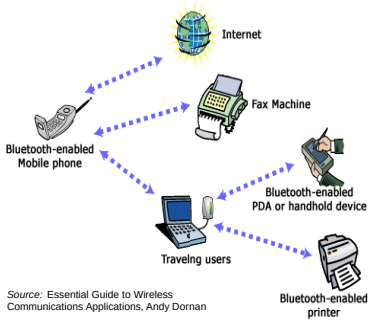


Figure 9.7
Scatternet formed from seven piconets

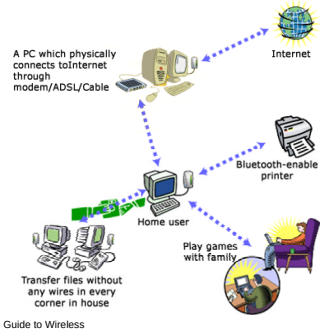
Source: Essential Guide to Wireless Communications Applications, Andy Dornan

Modèle – Utilisateur Mobile



Source: Essential Guide to Wireless Communications Applications, Andy Dornan

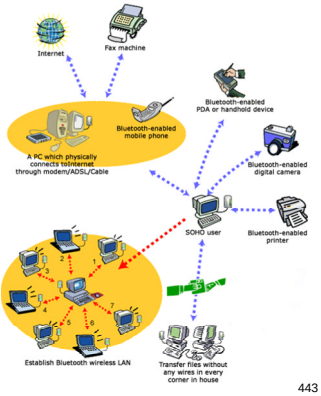
Modèle – Utilisateur à Domicile



Source: Essential Guide to Wireless Communications Applications, Andy Dornan

Modèle – Utilisateur SOHO Avancé

SOHO : Small Or Home Office

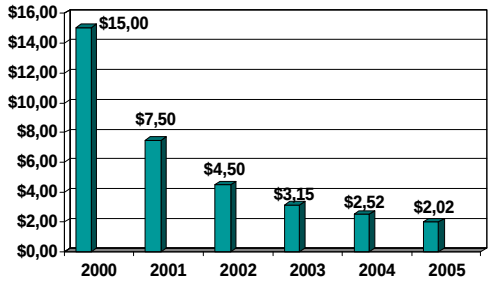


Source: Essential Guide to Wireless Communications Applications, Andy Dornan

Avantages de Bluetooth

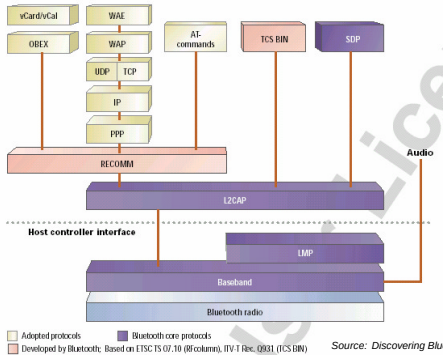
- Faible coût initial
- Synchronisation des réseaux ad hoc
- Puce radio de faible puissance
- Angle de connexions
- Réception des communications de données et de voix

Coûts des Puces Bluetooth



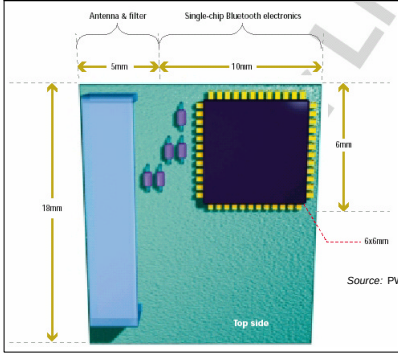
Source: Discovering Bluetooth, by M Miller

Pile de protocoles Bluetooth



Source: Discovering Bluetooth, by M Miller

Module Typique Bluetooth



Source: PWC 2000 Technology Forecast

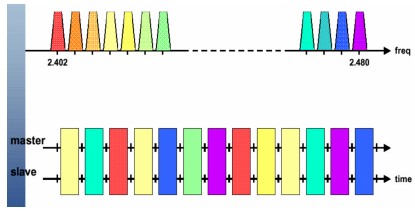
Caractéristiques

- Fréquences comprises entre 2,400 et 2,4835 GHz
- Débit théorique de 1 Mb/s (Bluetooth 2 : 12 Mbit/s)
- Classe de puissance
  - Classe 1: 100 mW (+20dBm max à 0 dBm w/ power control)
  - Classe 2: 2.5 mW (+ 4 dBm à -6 dBm)
  - Classe 3: 1 mW (0 dBm max)

Caractéristiques

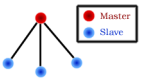
- Encryption sur 128-bit
- IEEE Standard - 802.15 (PAN)
- Immunité aux bruits et interférences provenant de technologies autres
  - CDMA - Changement de fréquences rapides (1600 hops/sec)
  - Petit paquet de données (2871 bits)
  - Contrôle de puissance
  - Correction d'erreurs (1/3 FCE, 2/3 FEC ou aucun)
  - Détection d'erreurs (CRC 8 ou 16 bits sur le message)

CDMA - Saut de fréquences

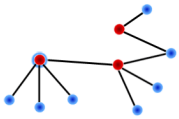


Schémas de connexion

Le plus simple des schémas de connexion est établi lors de la communication entre 2 périphériques bluetooth. Un des deux appareils jouera le rôle de Maître (**M**aster) et l'autre d'esclave (**S**lave). Le maître est chargé de gérer la communication entre les deux périphériques : c'est lui qui initialise la connexion.

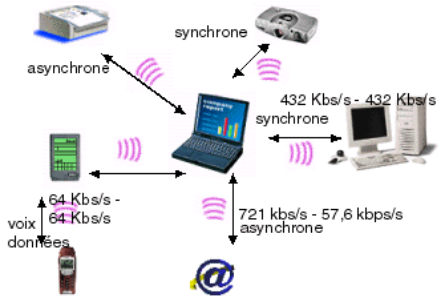


Dans le cas où plus de 2 périphériques se connectent au sein du même piconet, un des appareils devient maître et les autres esclaves. Le maître est alors chargé de gérer les communications entre les différents esclaves : lorsque 2 esclaves souhaitent échanger des informations, cette discussion est orchestrée par le maître.



Comme il a été indiqué plus haut, plusieurs piconets peuvent se réunir pour former un scatternet. Dans ce cas, le maître d'un piconet deviendra l'esclave du maître d'un autre piconet. Un périphérique pourra également devenir l'esclave de plusieurs maîtres de différents piconets, comme le montre le shcéma ci-dessus.

Modes de communication

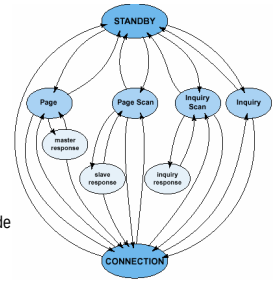


Établissement de la communication

Inquiry
- Search pour modules connus
- Modules peuvent répondre ou pas

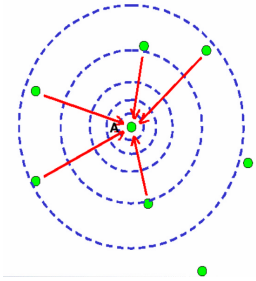
Page
- Établissement d'une connexion
- Un module à la fois
- Paging modules deviennent Master

Connect (choix de type de liens)
- **ACL**: asynch connectionless (paquet de données)
- **SCO**: synch connection-oriented (circuit de voix)



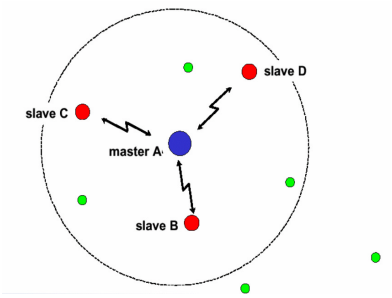
Établissement de la communication

Inquiry



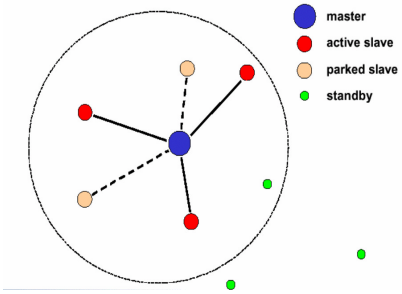
Établissement de la communication

Page



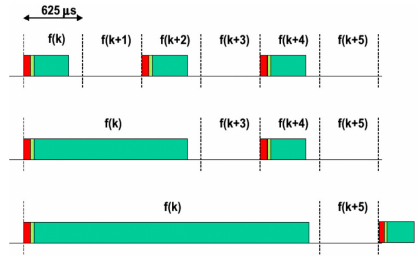
Établissement de la communication

États opérationnels



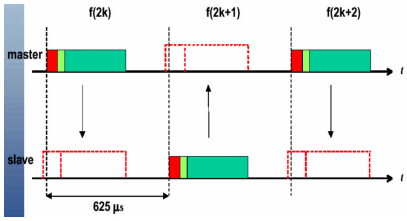
Paquet de données

Paquets de données 'Multi-Slots'

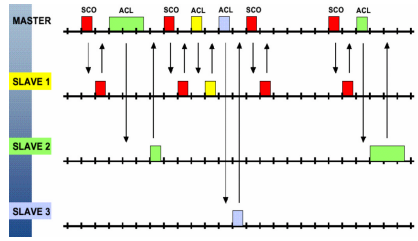


Mécanisme de réservation pour les paquets "multi-slots"

Canaux FH/TDD



Exemple de liens mixtes



Alternatives à Bluetooth

Source: Discovering Bluetooth, by M Miller

	Bluetooth	HomeRF	IEEE 802.11b (Wi-Fi)	IrDA
Primary Use	Cable replacement and ad hoc device-to-device connections	Home or small office LANs	Corporate or campus LANs	Cable replacement and ad hoc device-to-device connections (narrow angle)
Max Speed	1 Mbps	10 Mbps	11 Mbps	4 Mbps
Range	30 feet	150 feet	300 feet	3 feet
Through walls	Yes	Yes	Yes	No
Requires base station	No	No	Yes	No
Interference susceptibility	Medium	Medium	High	None
Power Reqs	Low	High	High	Low
Cost to build	$8 now	$70-$120	$100-$300	$2

Systèmes sans fil

Source: Discovering Bluetooth, by M Miller

Standard	Standards Body/Proponent	Frequency Band	Max Data Rate	Range
Bluetooth	**Bluetooth SIG**	**2.4 GHz ISM***	**1 Mbps** **10 Mbps ? (BT 2.0)**	**10–100 m**
SWAP	**HomeRF Working Group**	**2.4 GHZ ISM**	**2 Mbps** **10 Mbps**	**50 m**
IEEE 802.11b	**IEEE**	**2.4 GHZ ISM**	**11 Mbps** **54 Mbps (802.11g)**	**50 m**
IEEE 802.15	**IEEE**	**2.4 GHz ISM**	**15.1: 1 Mbps (Bluetooth)** **15.3: 22 Mbps**	**10 m**
IEEE 802.11a	**IEEE**	**5 GHz UNII****	**54 Mbps**	**50 m**
HiperLAN/2	**ETSI BRAN*****	**5 GHz UNII**	**54 Mbps**	**50 m**
MMAC******	**ARIB**	**5 GHz UNII**	**54 Mbps**	**50 m**

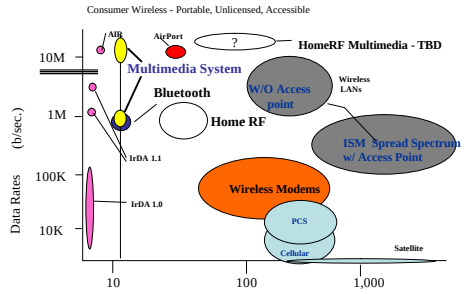
* Industrial, Scientific and Medical
** Unlicensed National Information Infrastructure
*** Broadband Radio Access Networks
**** Multimedia Mobile Access Communications

Fréquences et Modulations : comparaison

Source: Discovering Bluetooth, by M Miller

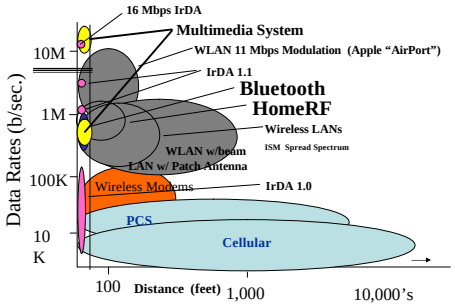
Parameters		Bluetooth	HomeRF		Upbanded DECT
Frequency					
Band		2.402 - 2.480 GHz	2.404 - 2.478 GHz		2.40 –2.483 GHz
Channel Spacing		1.000 MHz	1.000 MHz		³ 1.000 MHz
Accuracy		± 75 kHz	± 120 kHz		± 50 kHz
Lock time (est)		220 μsec	134 μsec		30 μsec (416.67 usec w/1 Blind slot)
Drift		± 40 kHz/ 5 slots	NA		± 40kHz/msec
Modulation					
Type		GFSK	2-FSK	(4-FSK)	GFSK
Deviation	Min	± 140 kHz	± 85 kHz	± 135 kHz	± 200 kHz nom.
	Max	± 175 kHz	± 177.5 kHz	± 190 kHz	(± 250 kHz nom)
Burst Bit Rate		1 Mbits/s	1 Mbit/s	2Mbit/s	1.152Mbits/s (1.0Mbits/s)
Accuracy		+/- 20ppm	+/- 50 ppm	+/- 9 ppm	N/A

Bande Passante vs Distance



Source: Jim Kardach, Intel

Bande Passante vs Distance



Source: Jim Kardach, Intel

IP Mobile