Les réseaux sans-fils

C. Pham
Université de Pau et des Pays de l'Adour
Département Informatique
http://www.univ-pau.fr/~cpham
Congduc.Pham@univ-pau.fr

Remerciements

- Les transparents de ce cours ont été gracieusement prêtés par F. Dupond de l'université Claude Bernard, Lyon 1

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)

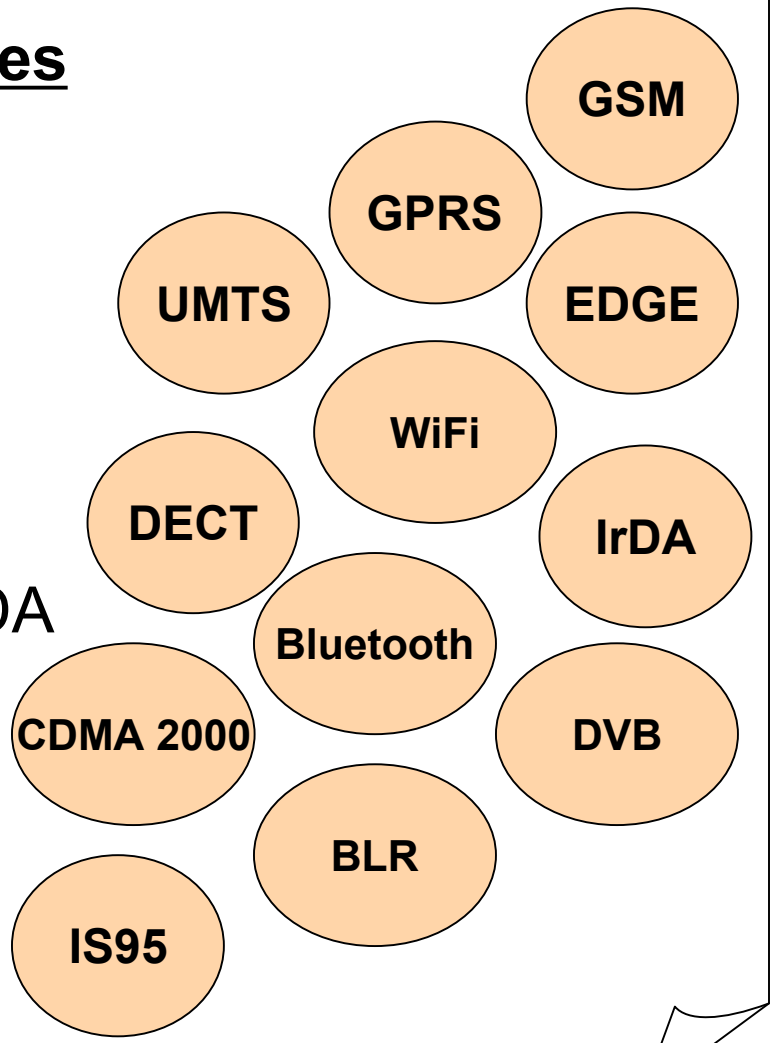
1ère partie

- 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 : 1èreliaison téléphonique transcontinentale (Bell System)
- 1930 : Télévision (principes)

Historique

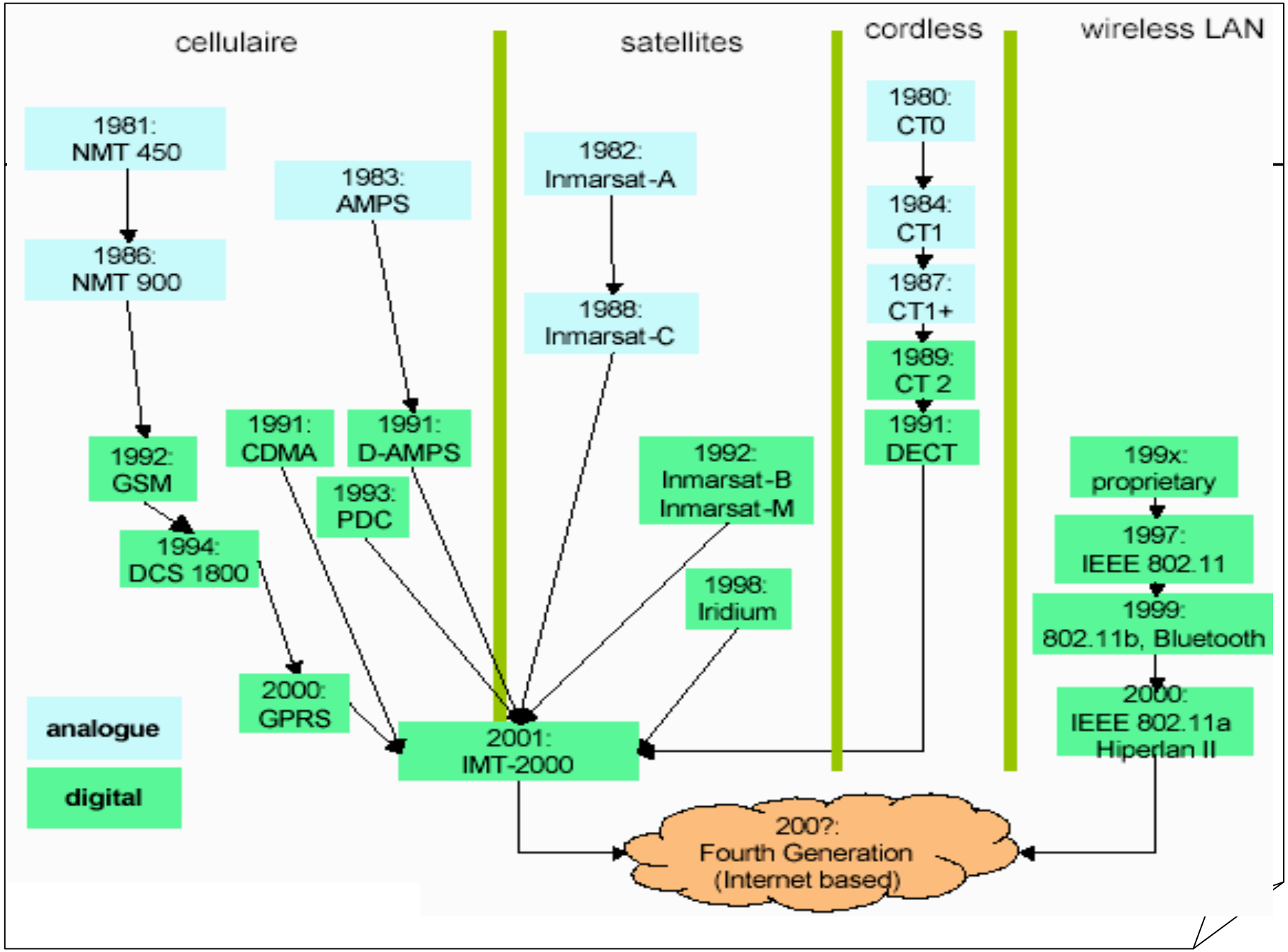
- 1948 : Invention du transistor, théorie de Shannon
- 1950 : nombreuses communications mobiles professionnelles
- 1958 : 1er réseau cellulaire public (Allemagne)
- 1962 : 1er satellite TV (Telsar I)
- 1962 : 1er satellite géostationnaire (Intelsat I)
- 1964 : Transmission de données sur RTC
- 1969 :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

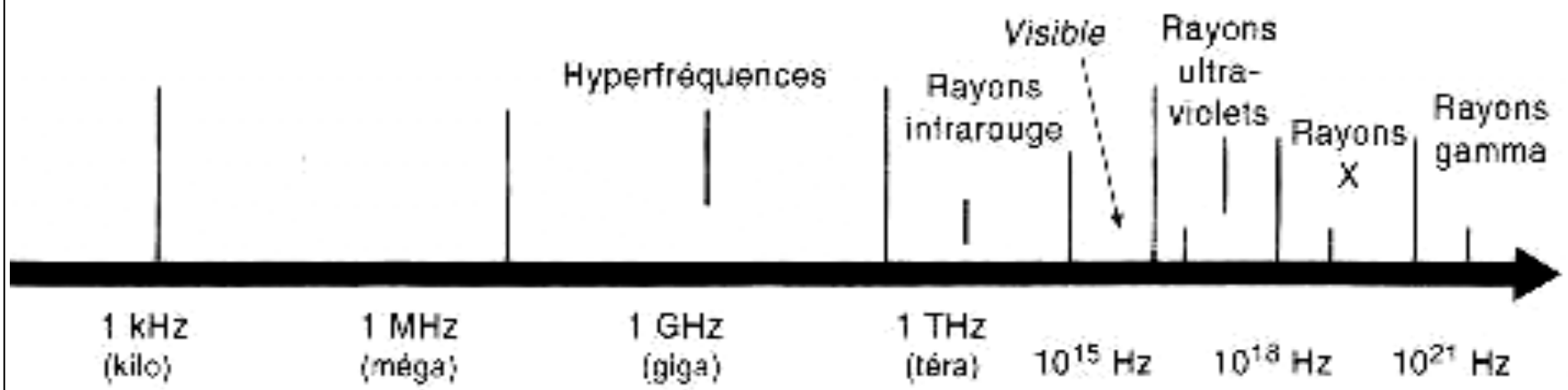
Développement du sans-fil

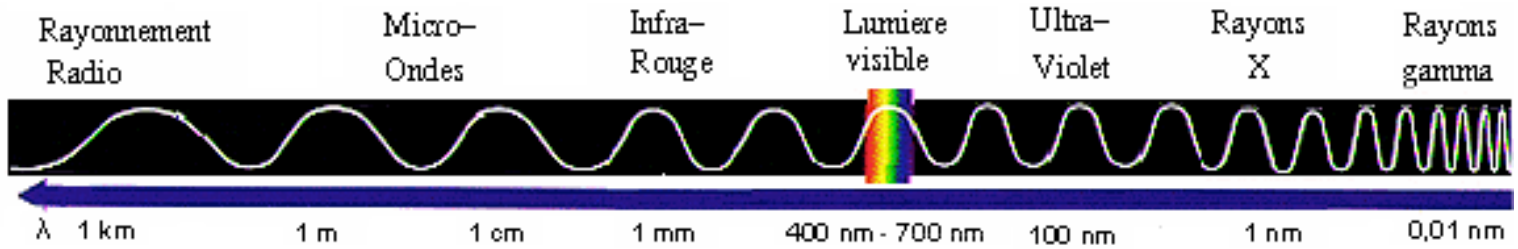
- La déréglementation a joué un rôle important…
- Progrès en électronique :
  - miniaturisation des équipements
  - augmentation de l'autonomie (batteries)
  - réduction du prix des équipements
- Moyen le plus rapide et le moins coûteux pour couvrir un territoire sans "re-câbler"
- Intérêt de la mobilité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


cellulaire
satellites
cordless
wireless LAN
1981: NMT 450
1986: NMT 900
1992: GSM
1994: DCS 1800
2000: GPRS
1983: AMPS
1991: D-AMPS
1991: CDMA
1993: PDC
1982: Inmarsat-A
1988: Inmarsat-C
1992: Inmarsat-B Inmarsat-M
1998: Iridium
1980: CT0
1984: CT1
1987: CT1+
1989: CT 2
1991: DECT
199x: proprietary
1997: IEEE 802.11
1999: 802.11b, Bluetooth
2000: IEEE 802.11a Hiperlan II
2001: IMT-2000
200?: Fourth Generation (Internet based)
analogue
digital

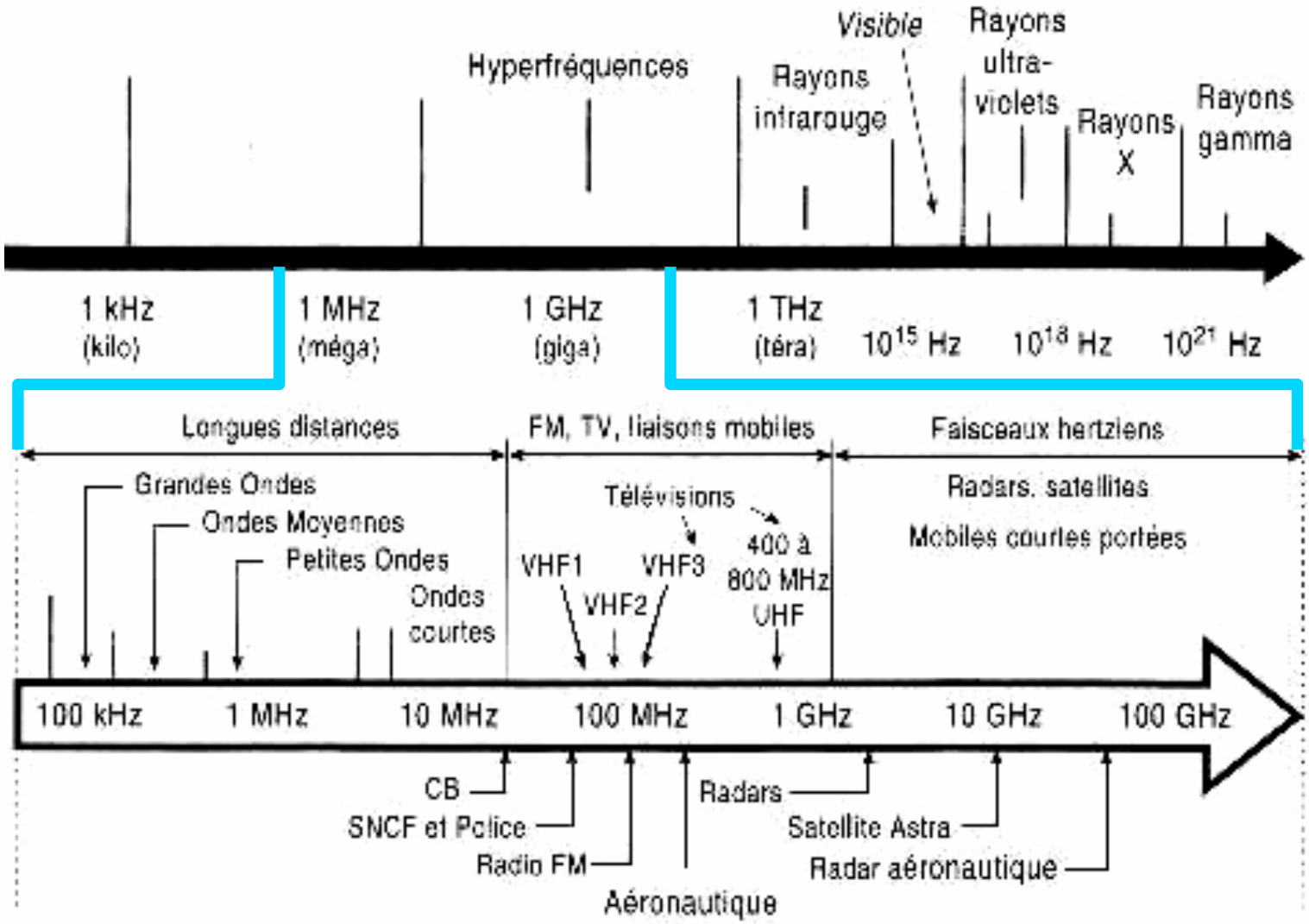
Utilisation des bandes de fréquences

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

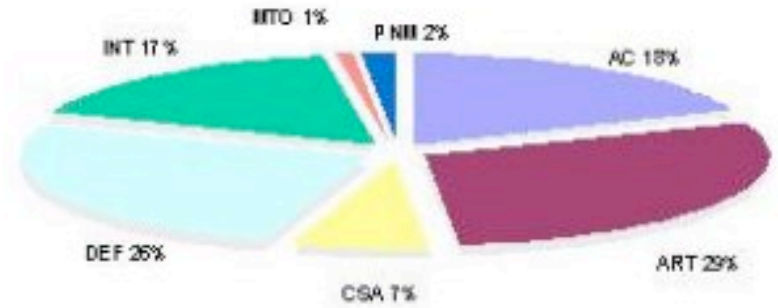
Agence nationale des fréquences (www.afnr.fr)

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

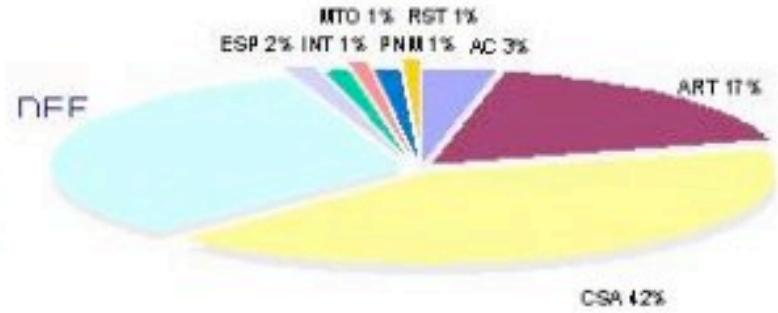
Bande des fréquences	2400 à 2454 MHz
Puissance max.	100 mW
Largeur canal	non imposée
Références	Décisions ART N°xxx

Répartition nationale des bandes de fréquences

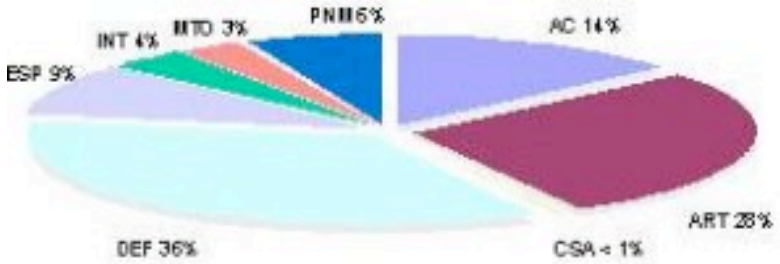
Bande 9 kHz – 29.7 MHz



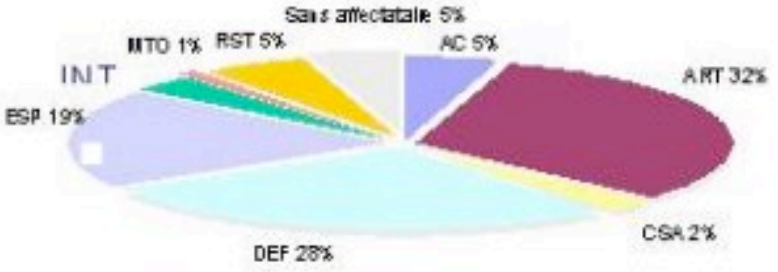
Bande 29.7 - 960 MHz



Bande 960 MHz -



Bande 10 GHz - 65 GHz



- Aviation civile (AC)
- Autorité de régulation des télécommunications (ART)
- Conseil supérieur de l'audiovisuel (CSA)
- Ministère de la défense (DEF)
- Espace (ESP)
- Ministère de l'intérieur (INT)
- Météorologie (MTO)
- Ports et navigation maritime (PNM)
- Radioastronomie (RST)

Propagation

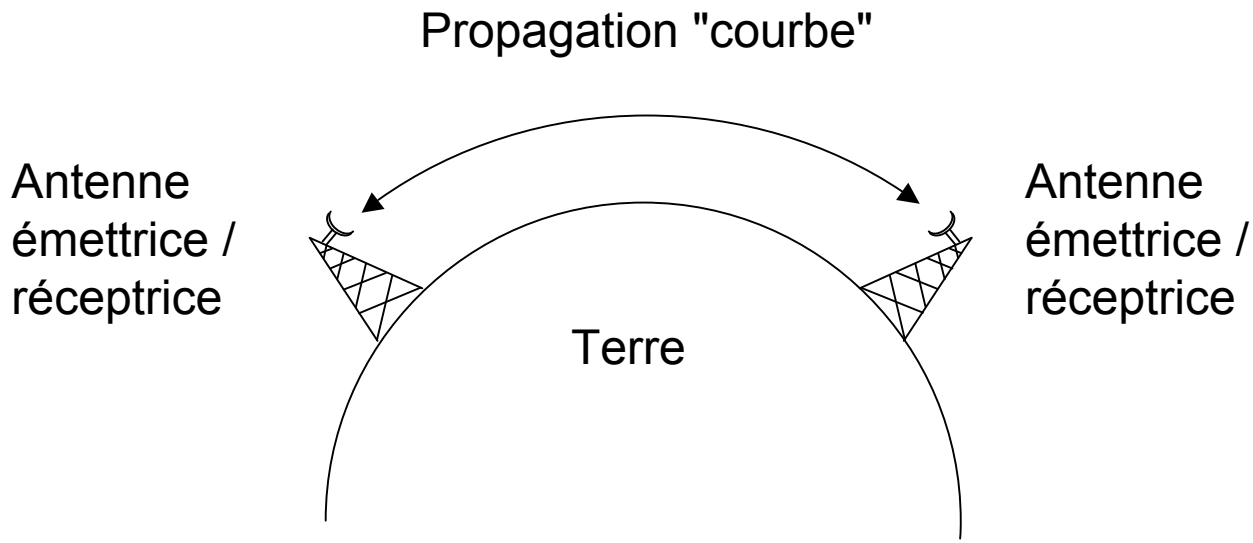
Gain d'antenne

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

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

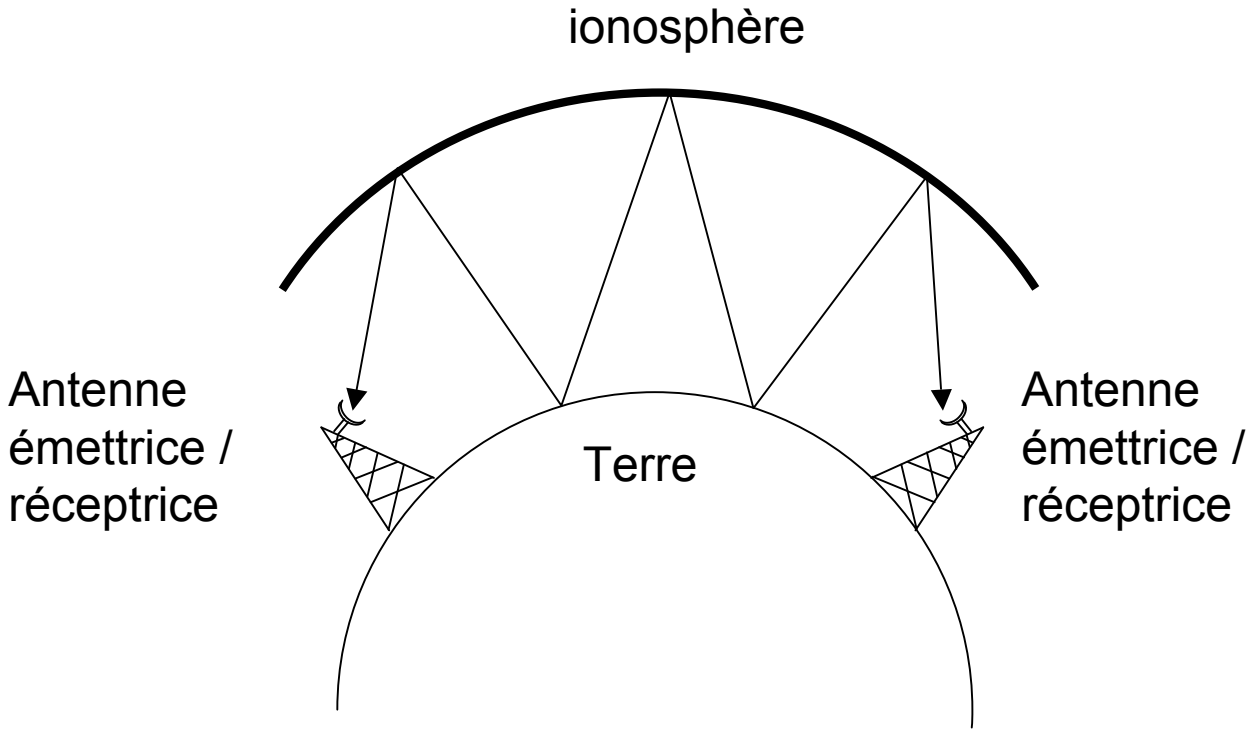
  - G = gain
  - A_e=surface effective
  - f = fréquence de la porteuse
  - c = vitesse de la lumière 3.10^8 m/s
  - λ= longueur d'onde de la porteuse

Propagation par onde de sol



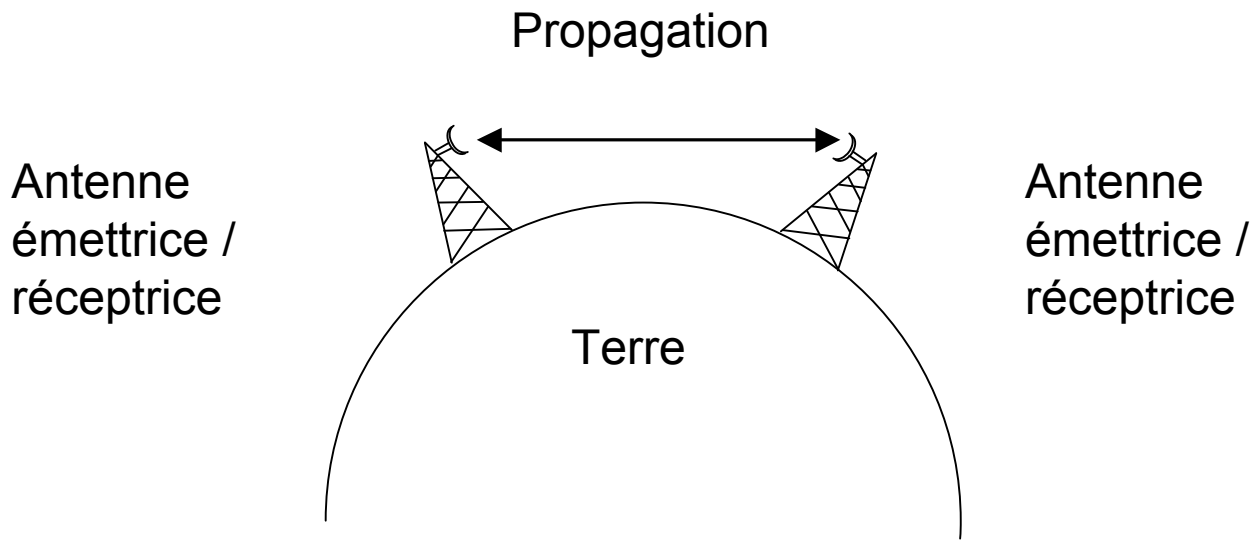
- Suit la courbure de la terre
- Grandes distances
- Fréquence -> 2 MHz
- Exemple Radio AM

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
  - α 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
  - λ= 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 :

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

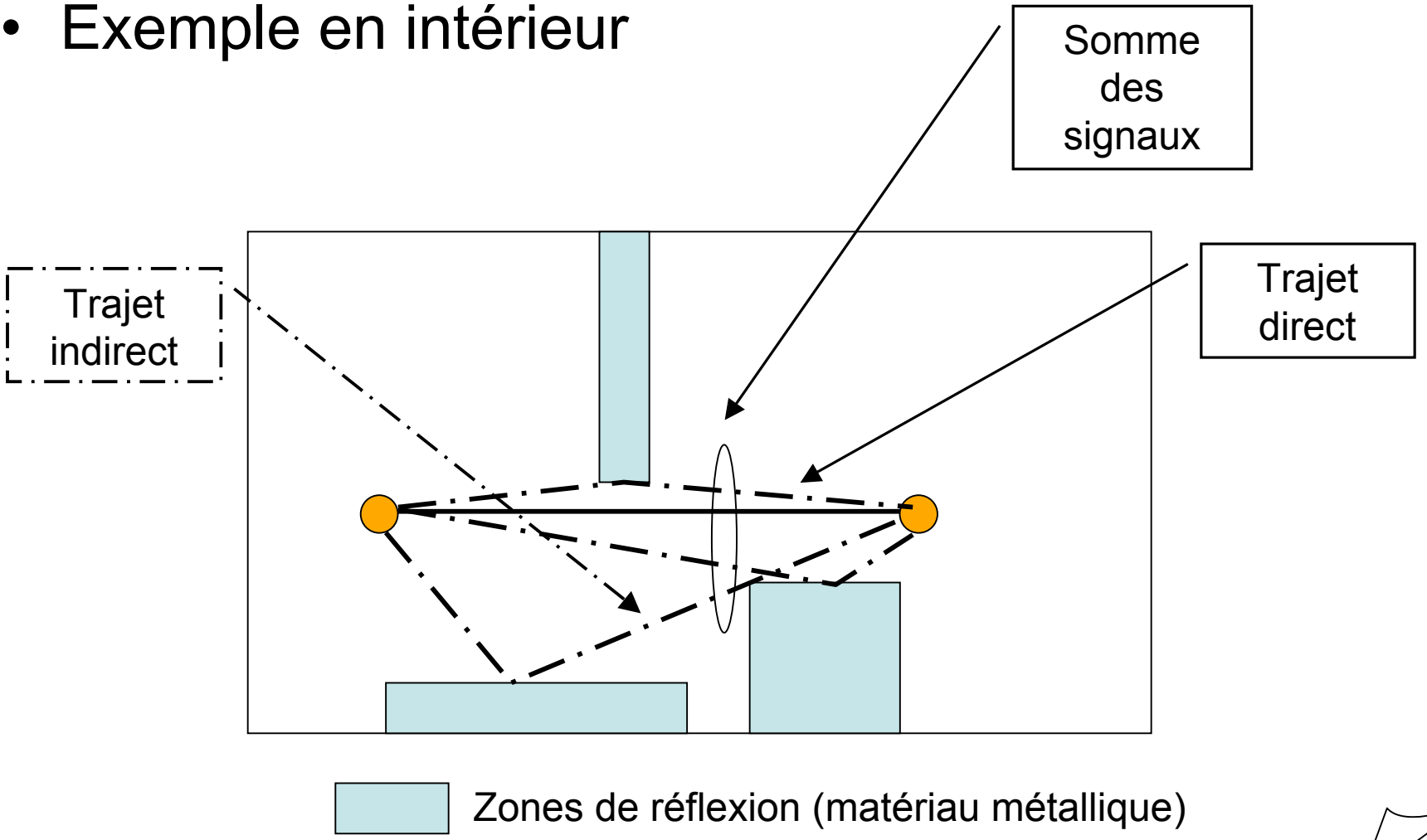
$$L_{(dB)} = 20\ log(\lambda) + 20\ log(d) - 10\ log(A_e A_r)$$

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

  - 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

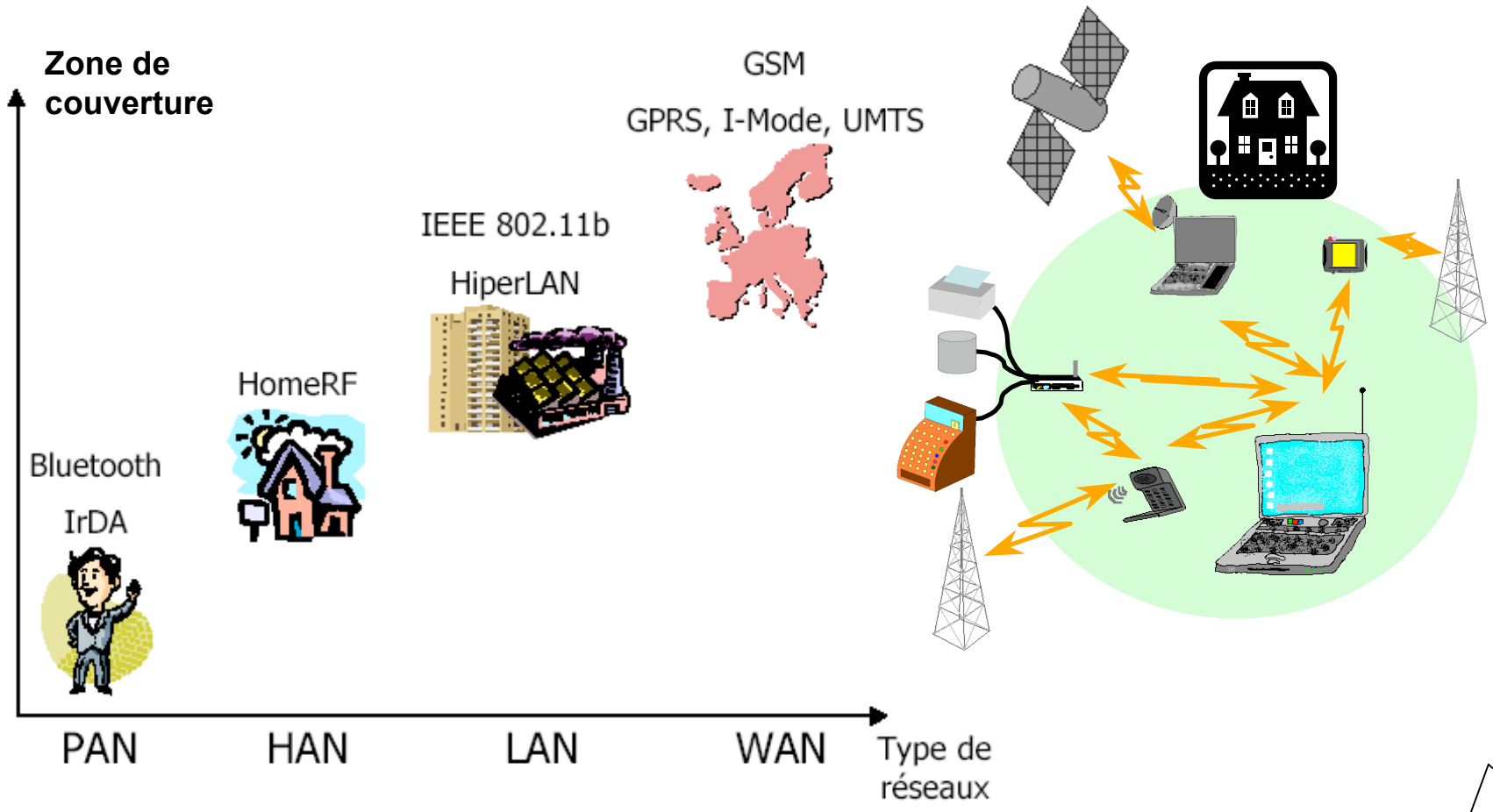
Notion de multi-trajets

- Exemple en intérieur



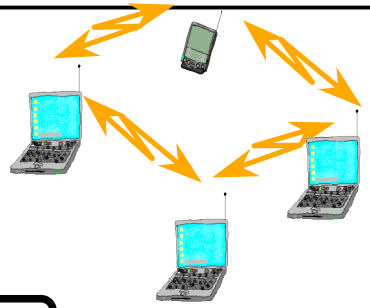
Types de réseaux sans fil

Couverture des réseaux sans fil



Couverture des réseaux sans fil

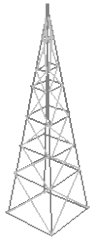
- **PAN** : Personal Area Network
  - ~ quelques mètres autour de l'usager
  - Ex : Bluetooth, IrDA

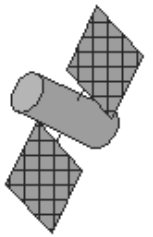


- **HAN** : Home Area Network
  - ~ 10 mètres autour d'une station relais
  - Ex : HomeRF

- **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

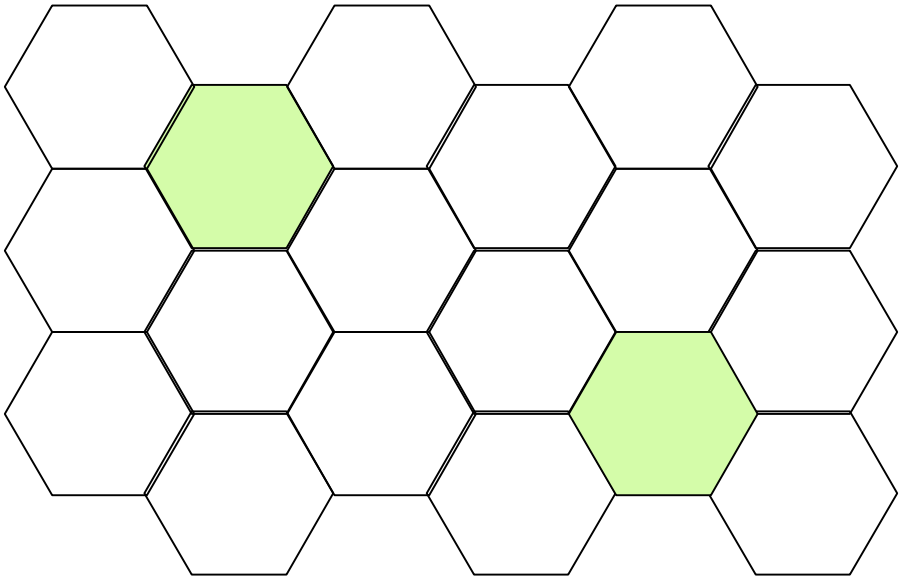
de taille variable :

  - 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)

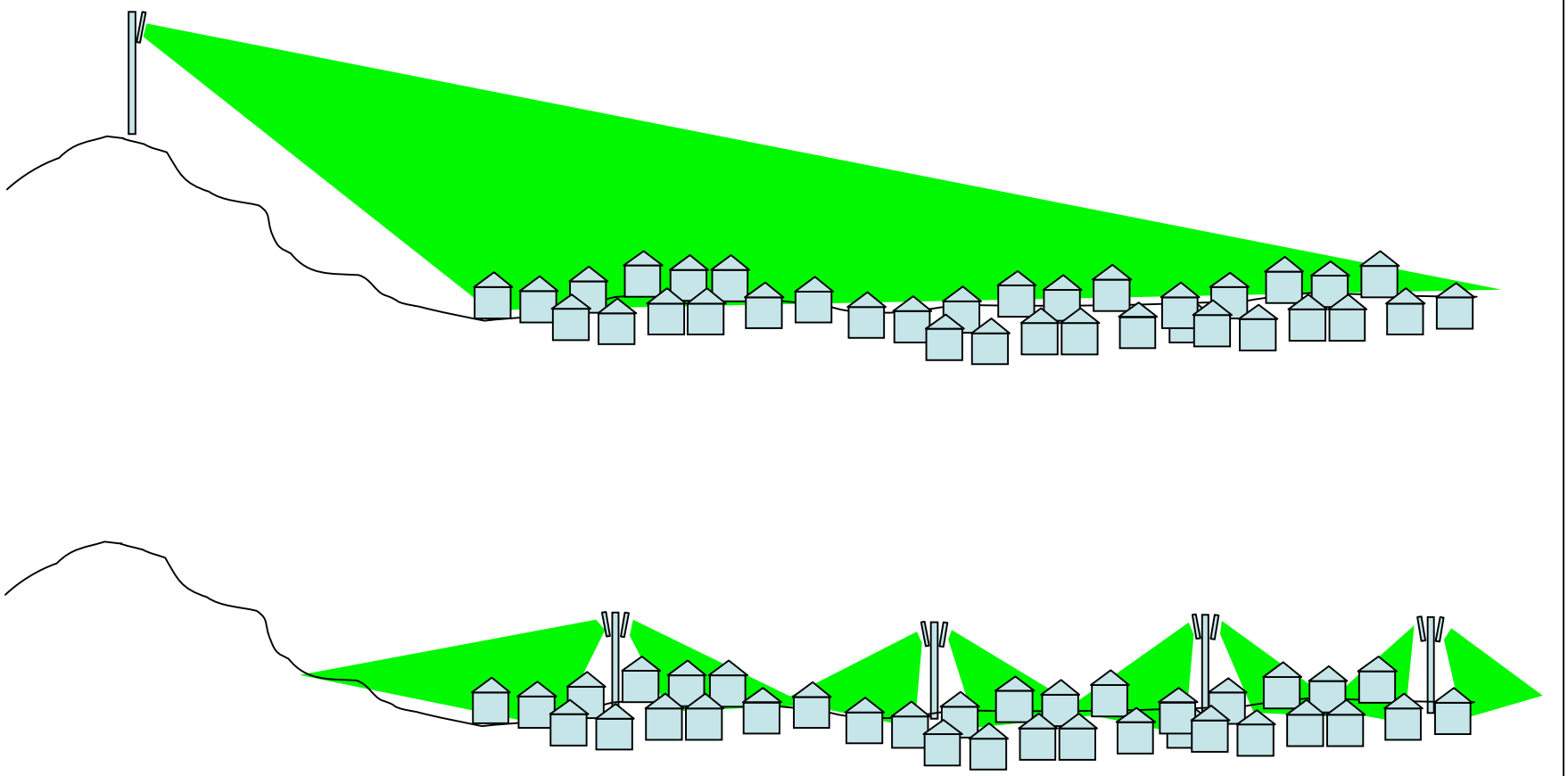
Organisation cellulaire

- Réutilisation de la même fréquence sur des zones géographiques différentes



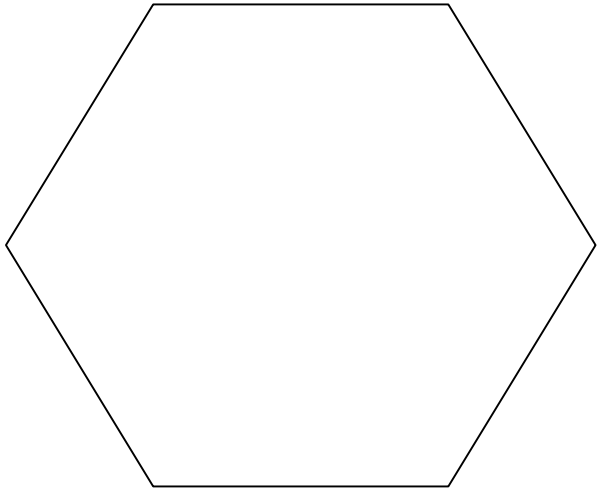
- Avantage : augmentation de la capacité
- Inconvénient : augmentation des interférences

Implantation des antennes

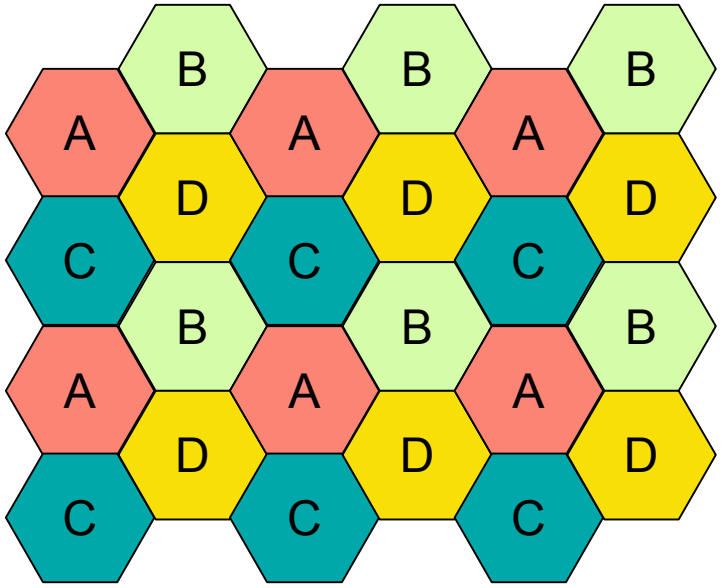


Exemple : couverture d'une zone

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

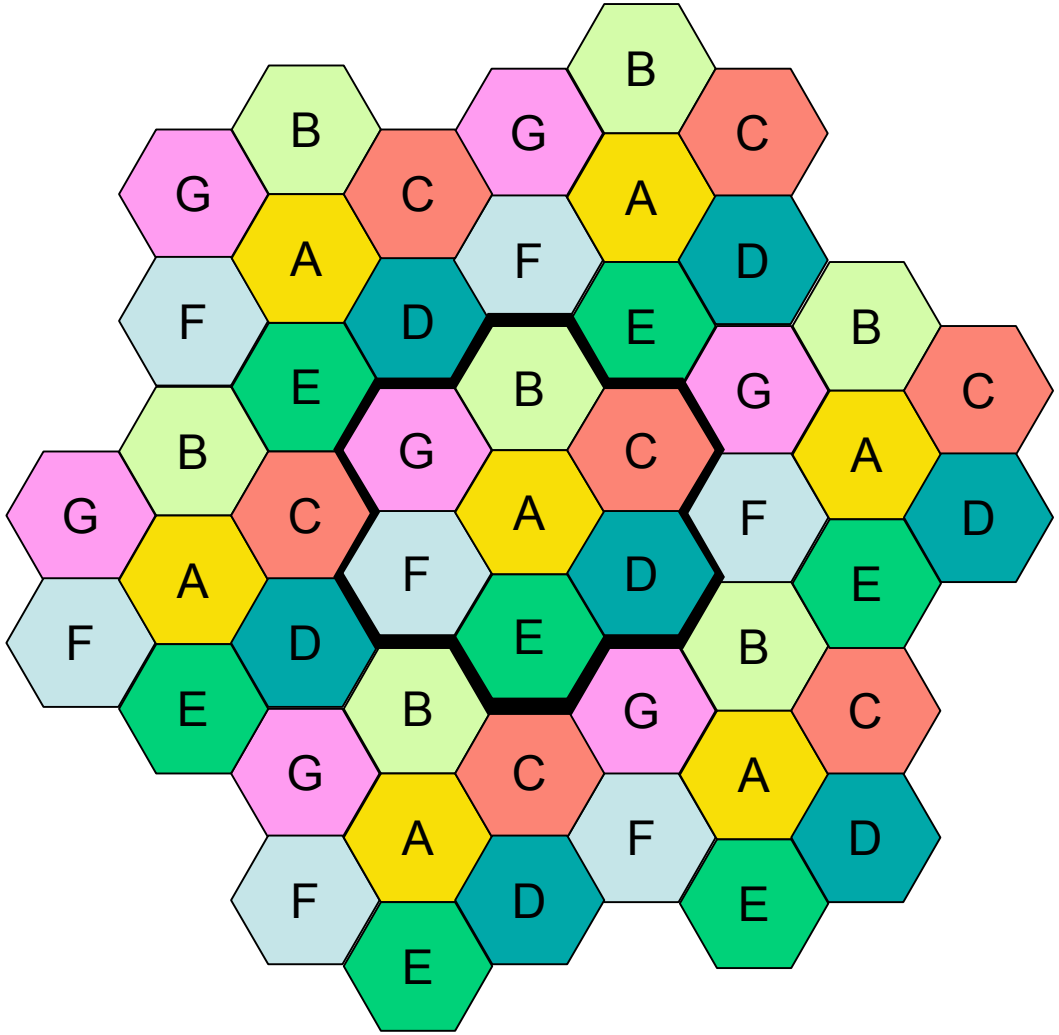
- Facteur de réutilisation

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

avec :

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

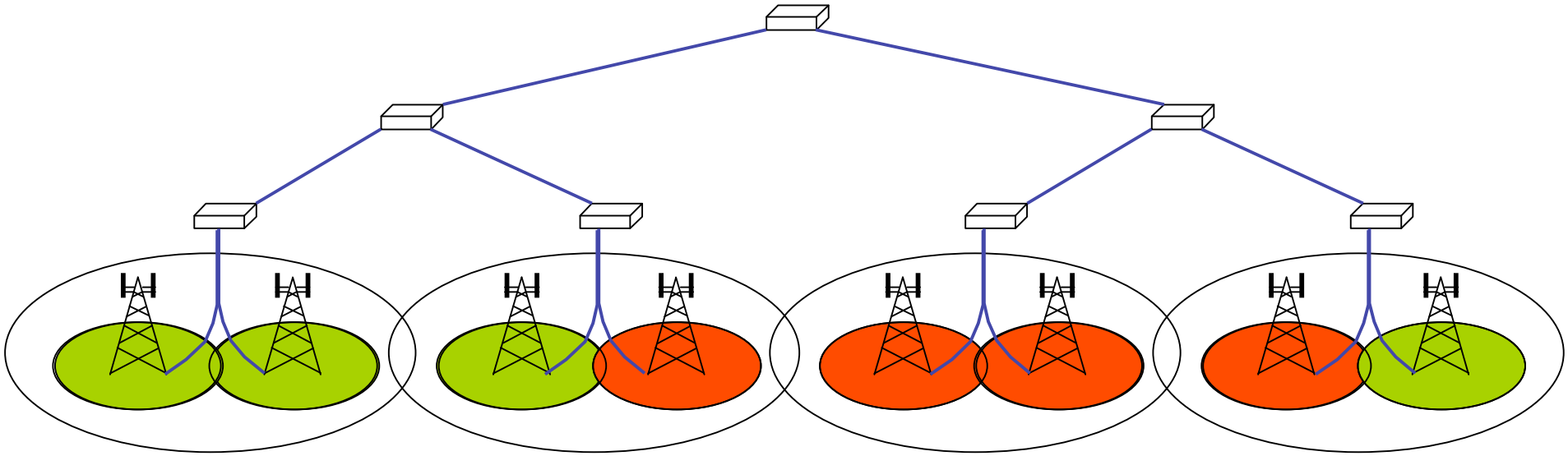
Exemple en zone urbaine, N=7



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"



En veille

En communication
Mécanisme de Handover

En veille

Mécanisme de "Handover"

- Objectif :
  - assurer la continuité des communications tout en assurant une certaine qualité de service.

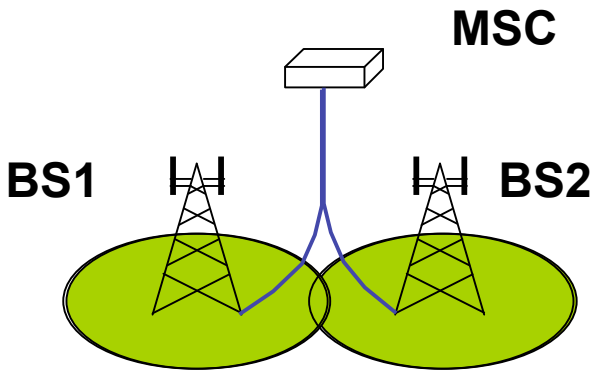
- Raisons :
  - optimiser l'utilisation des ressources
  - équilibrer le trafic entre cellules

➢ 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"

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 "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

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

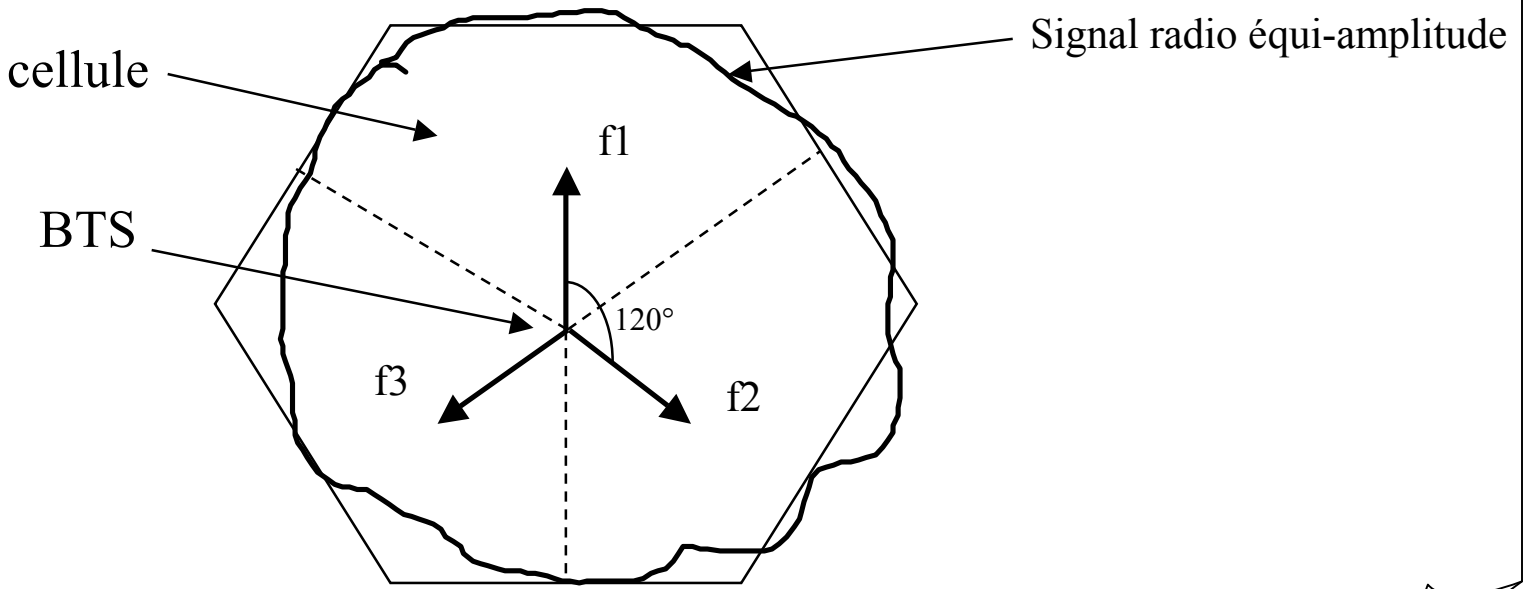
Cellule GSM

- 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

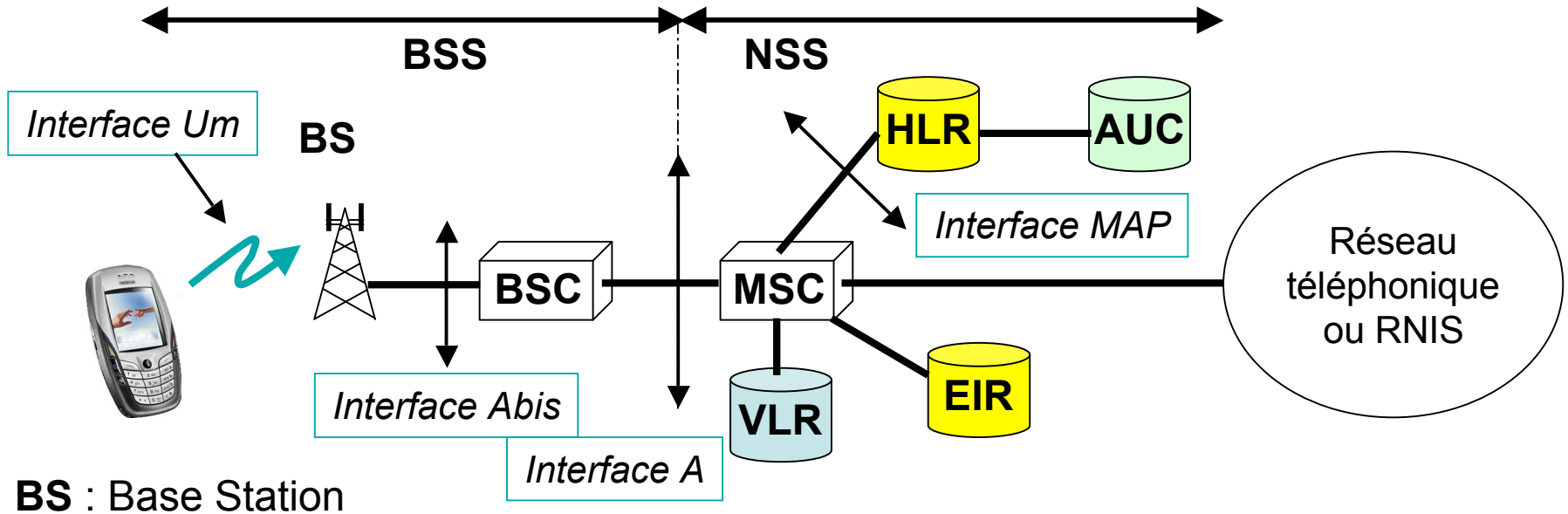
Cellule GSM

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

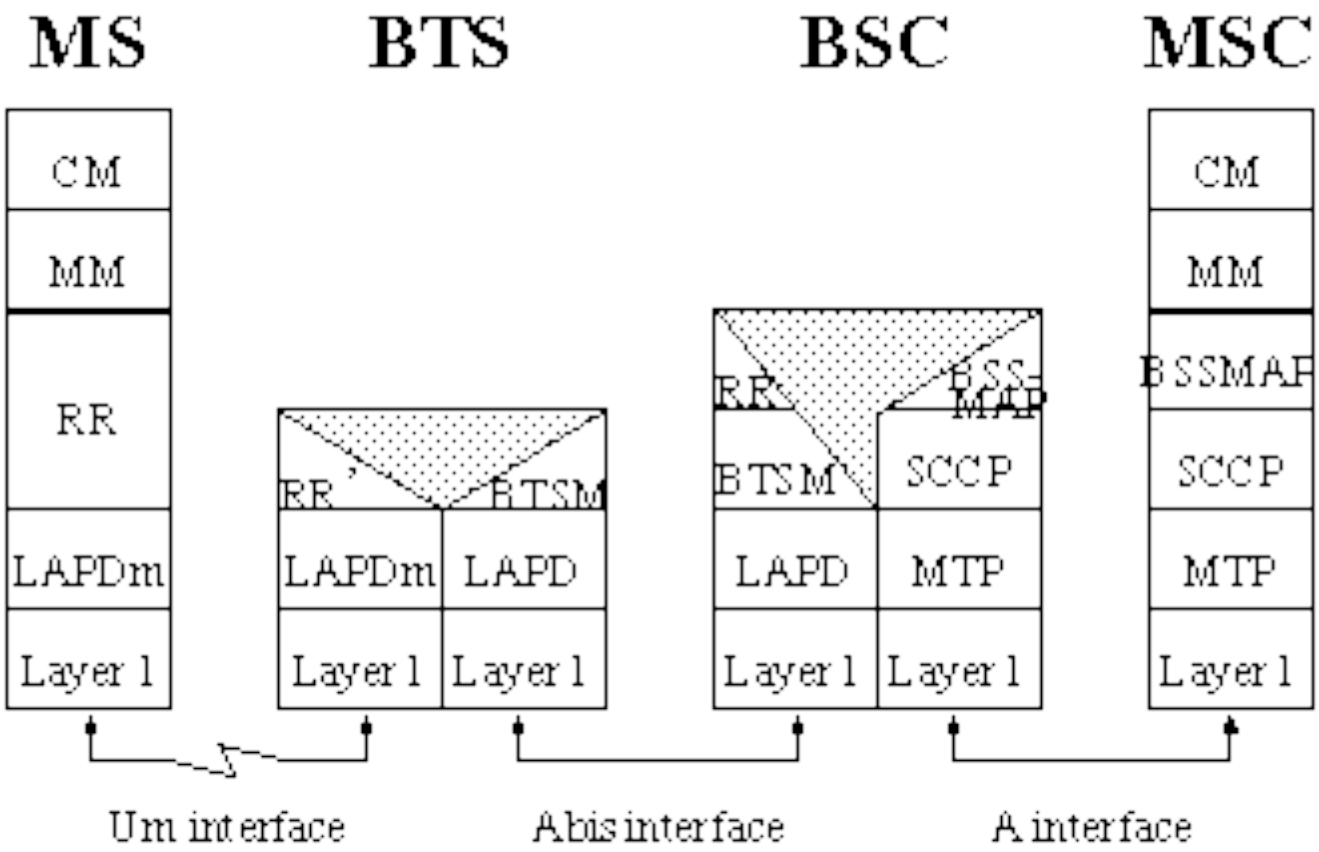
Operation and Maintenance Center

- 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

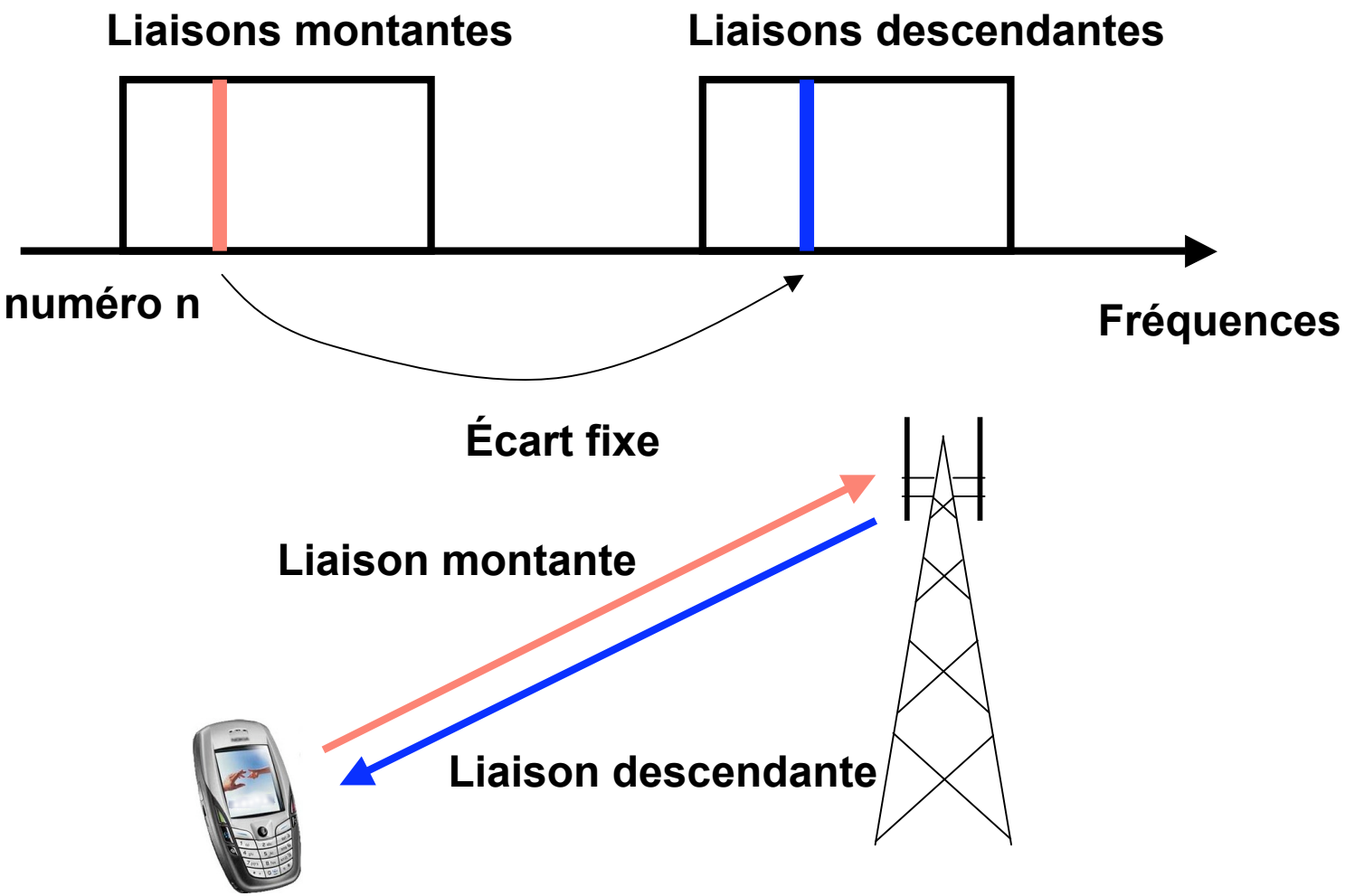
Interfaces et protocoles



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

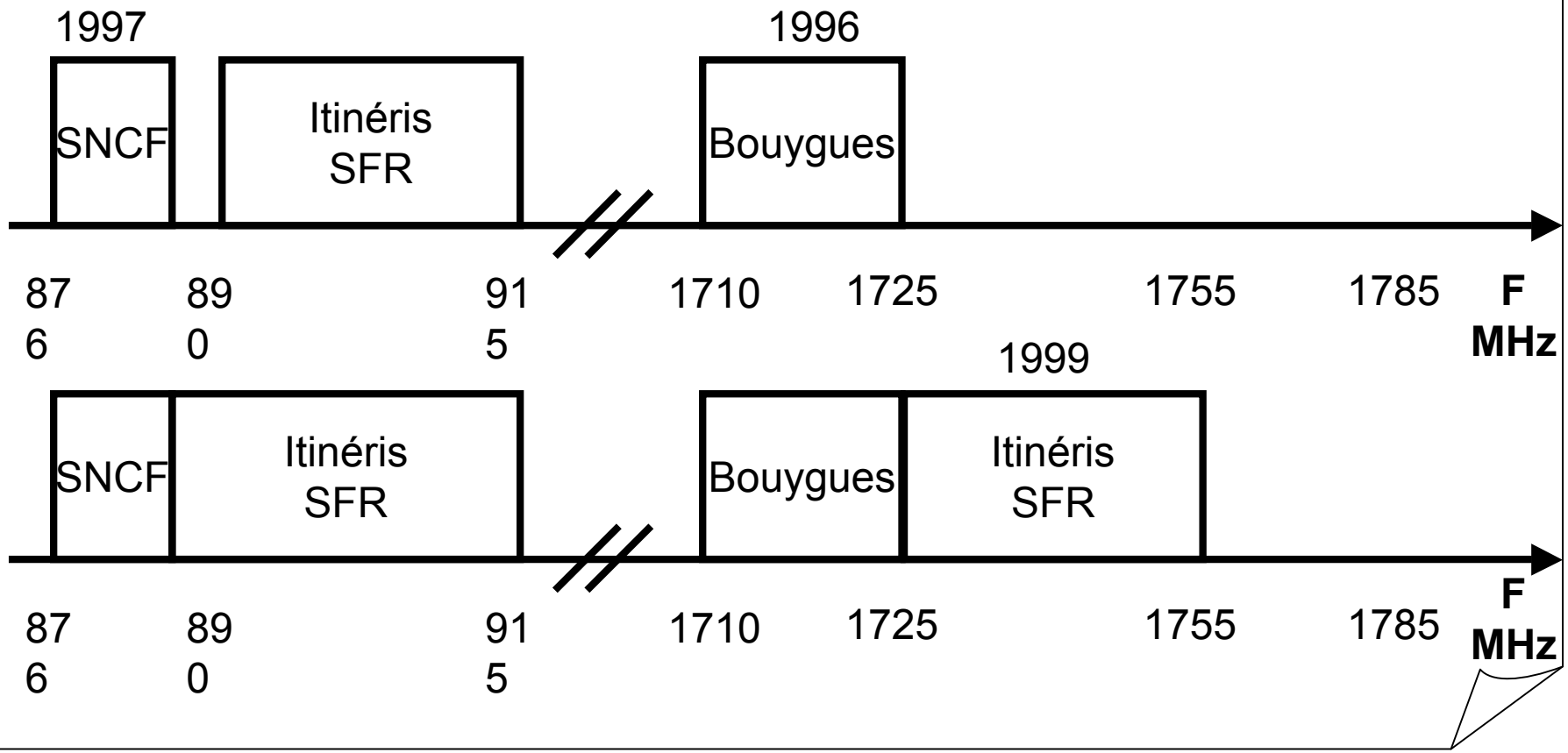

Liaisons montantes
Liaisons descendantes
numéro n
Fréquences
Écart fixe
Liaison montante
Liaison descendante

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

- 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

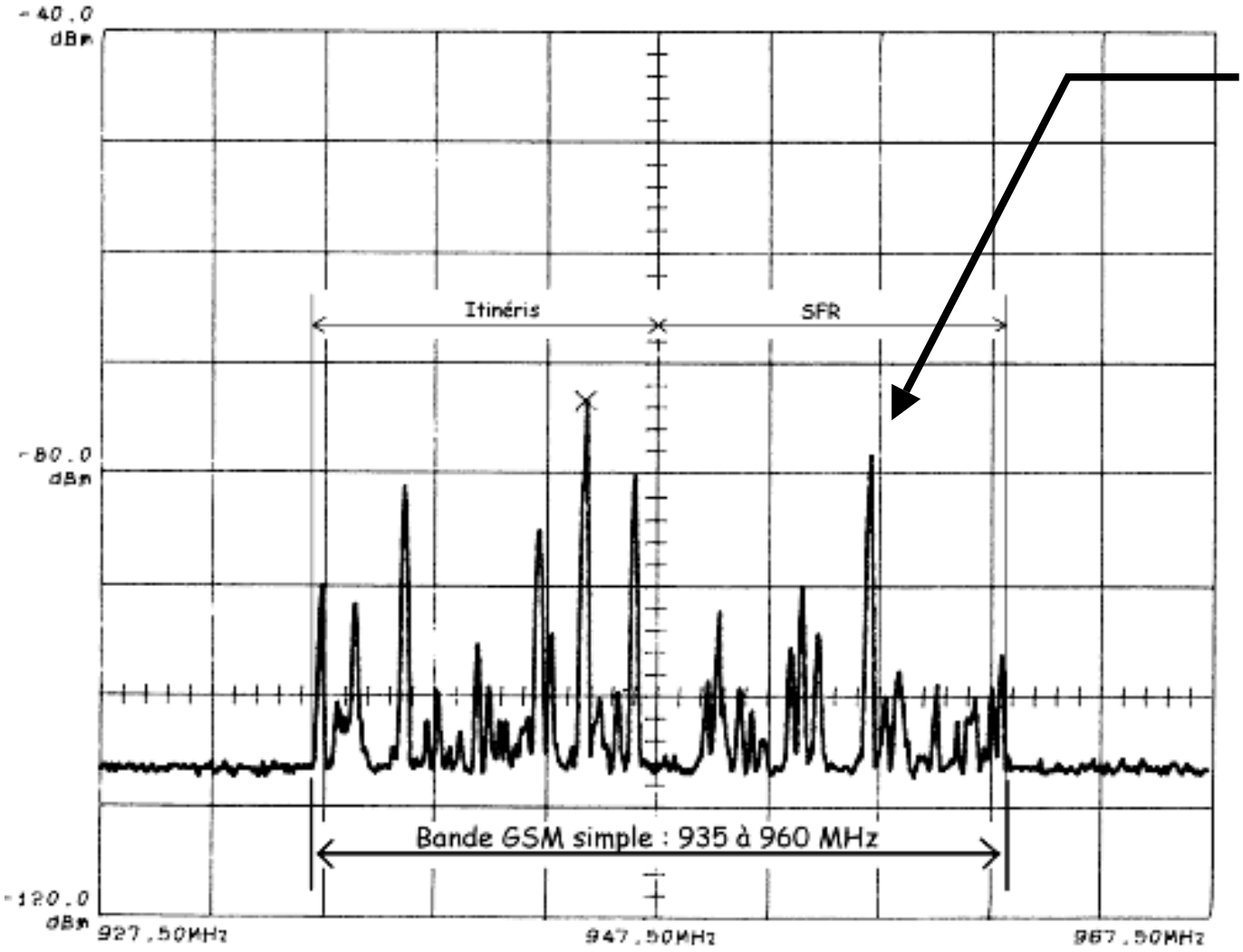
Mobile en veille :

- 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 :

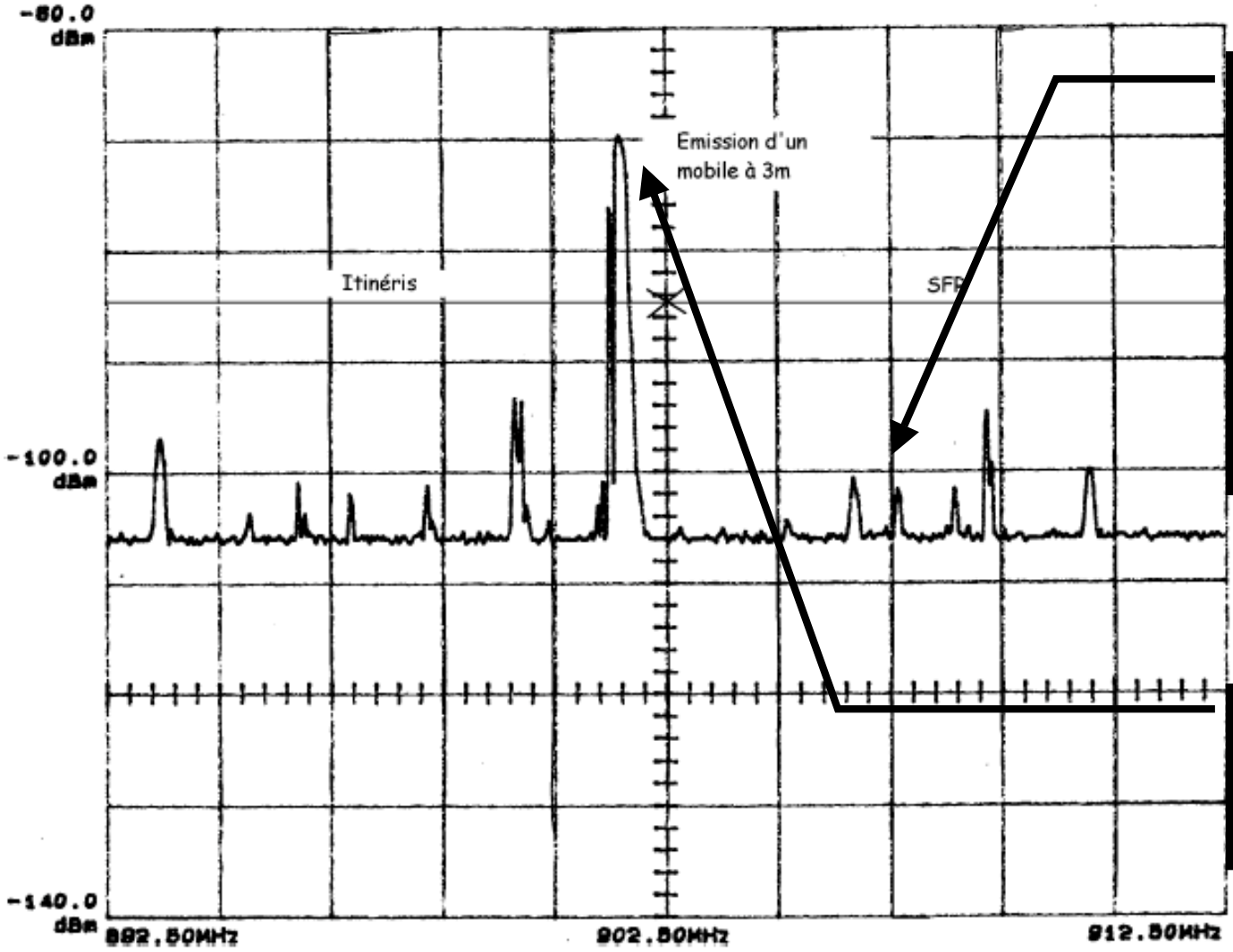
- Échange des signaux de parole et de contrôle sur la voie TCH (émission en slot i à f, réception en slot i à f+écart)
- Écoute des voies balises pour un éventuel changement de cellule

Spectre de la bande GSM descendante



Voie balise de la cellule la plus forte pour un opérateur

Spectre de la bande GSM montante

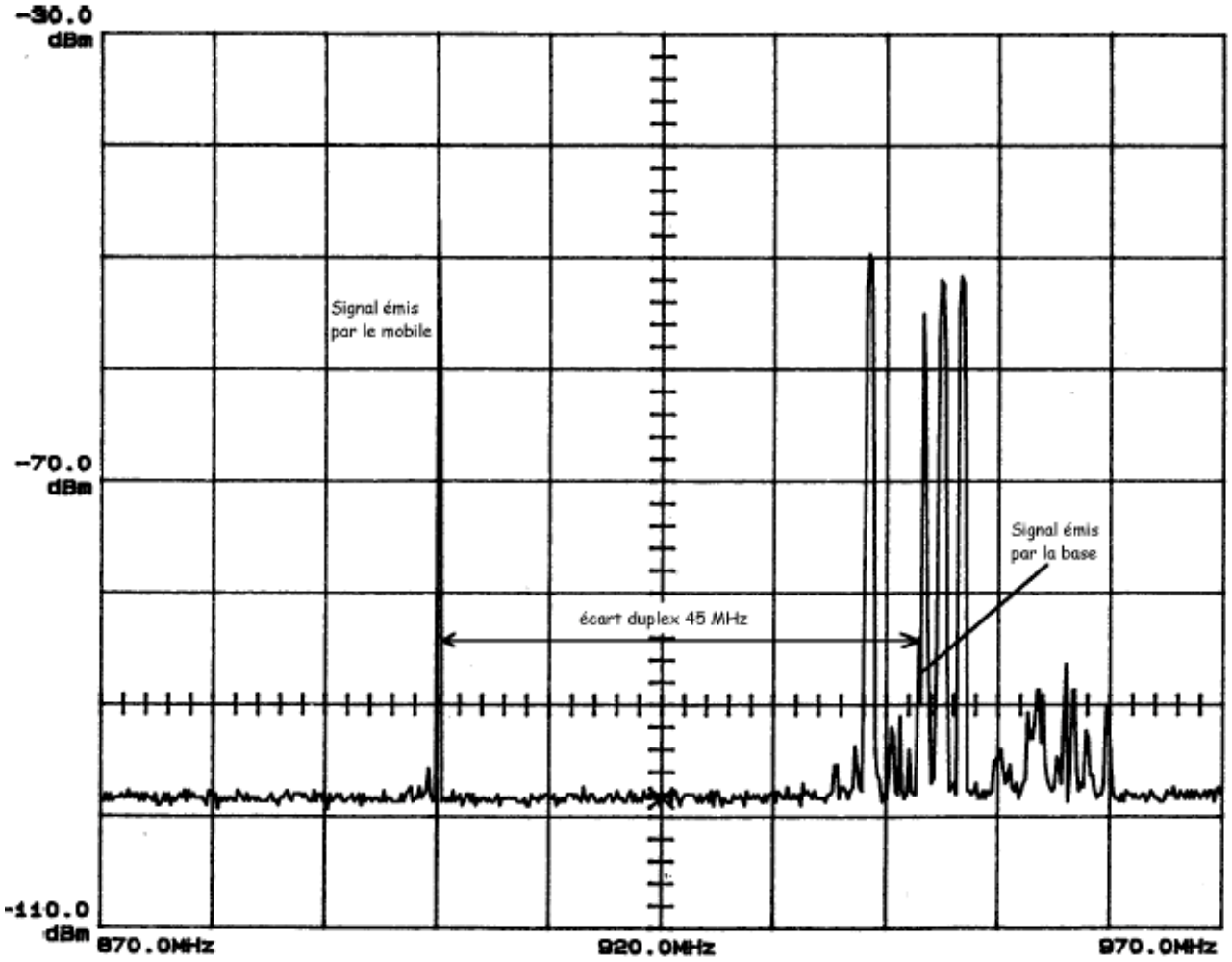


Pics : correspondent à l'allumage des mobiles

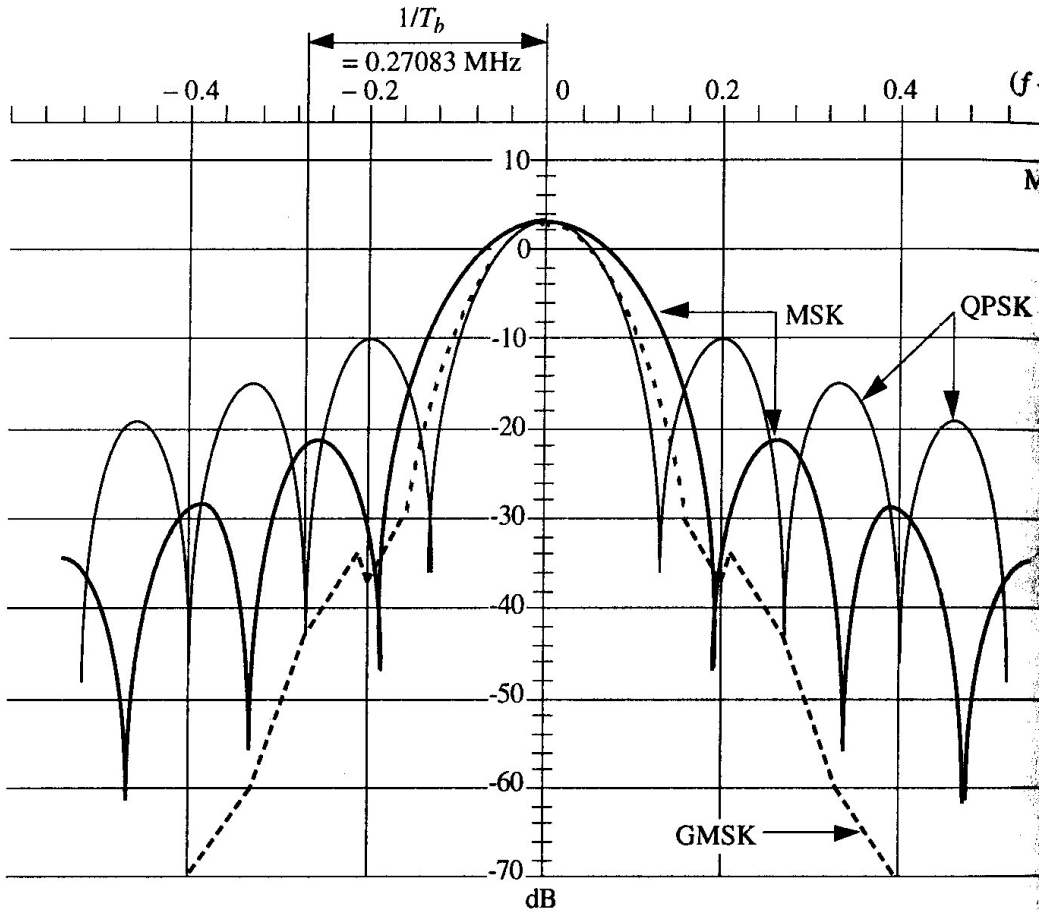
Superposition de 2h d'enregistrement

Communication proche de l'enregistreur

Spectres de la bande montante et descendante pendant une conversation



Modulation GMSK



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

Largeur de bande: 200 kHz

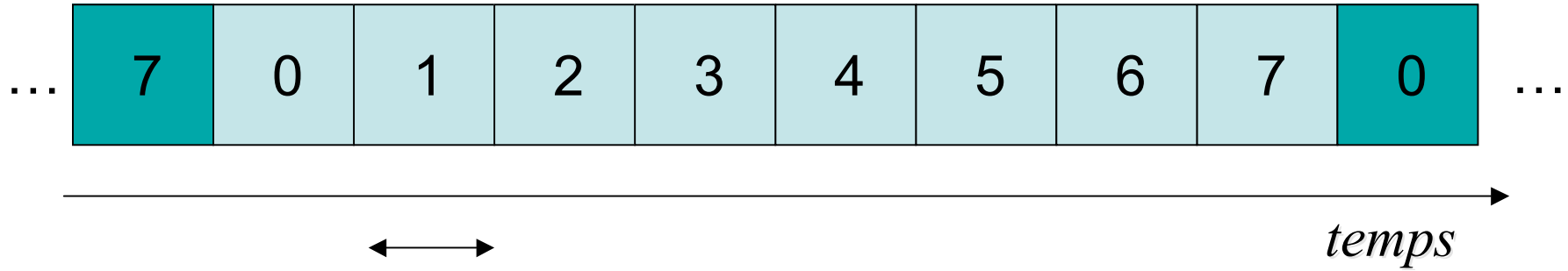
Débit binaire: 270.833 kbps

1 bit = 3.7 μs

Multiplexage temporel : TDMA

8 Time Slots par canal

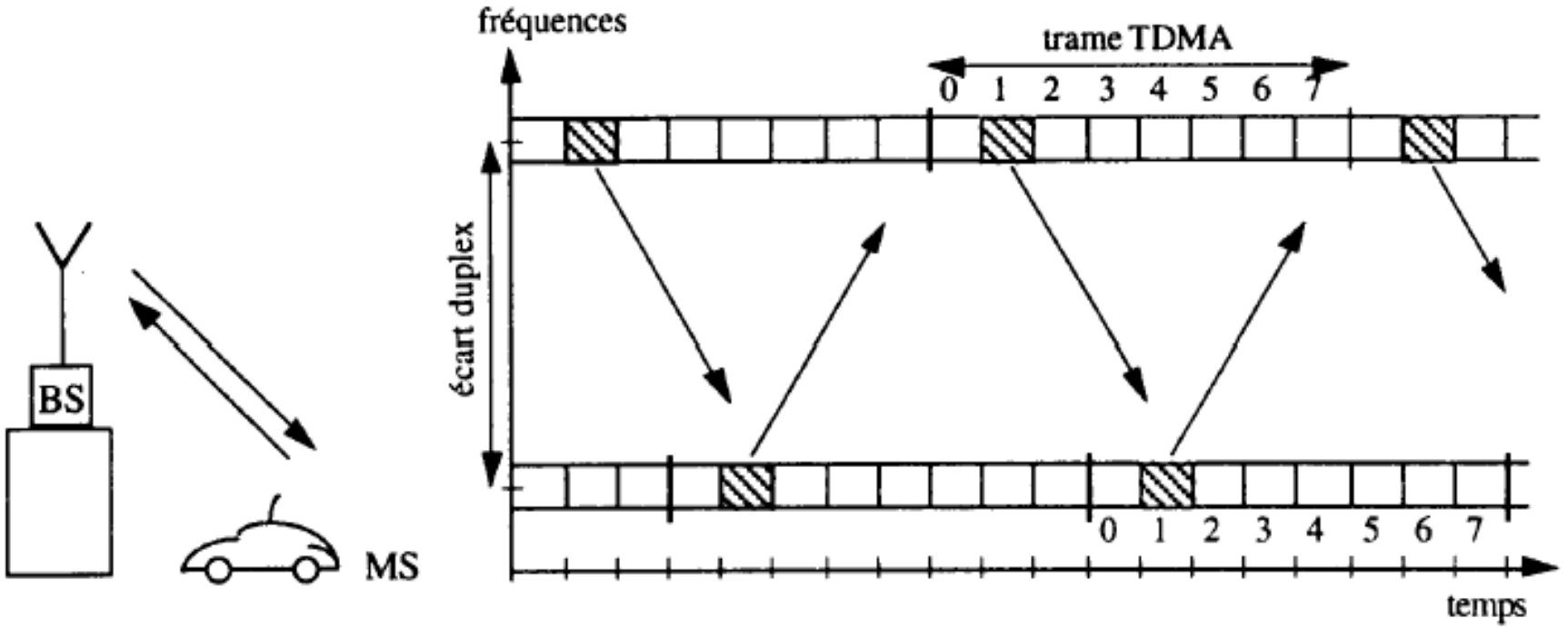
Durée d'une trame TDMA = 4.62 ms



7500 x 1/13 MHz = **577 µs**
(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.

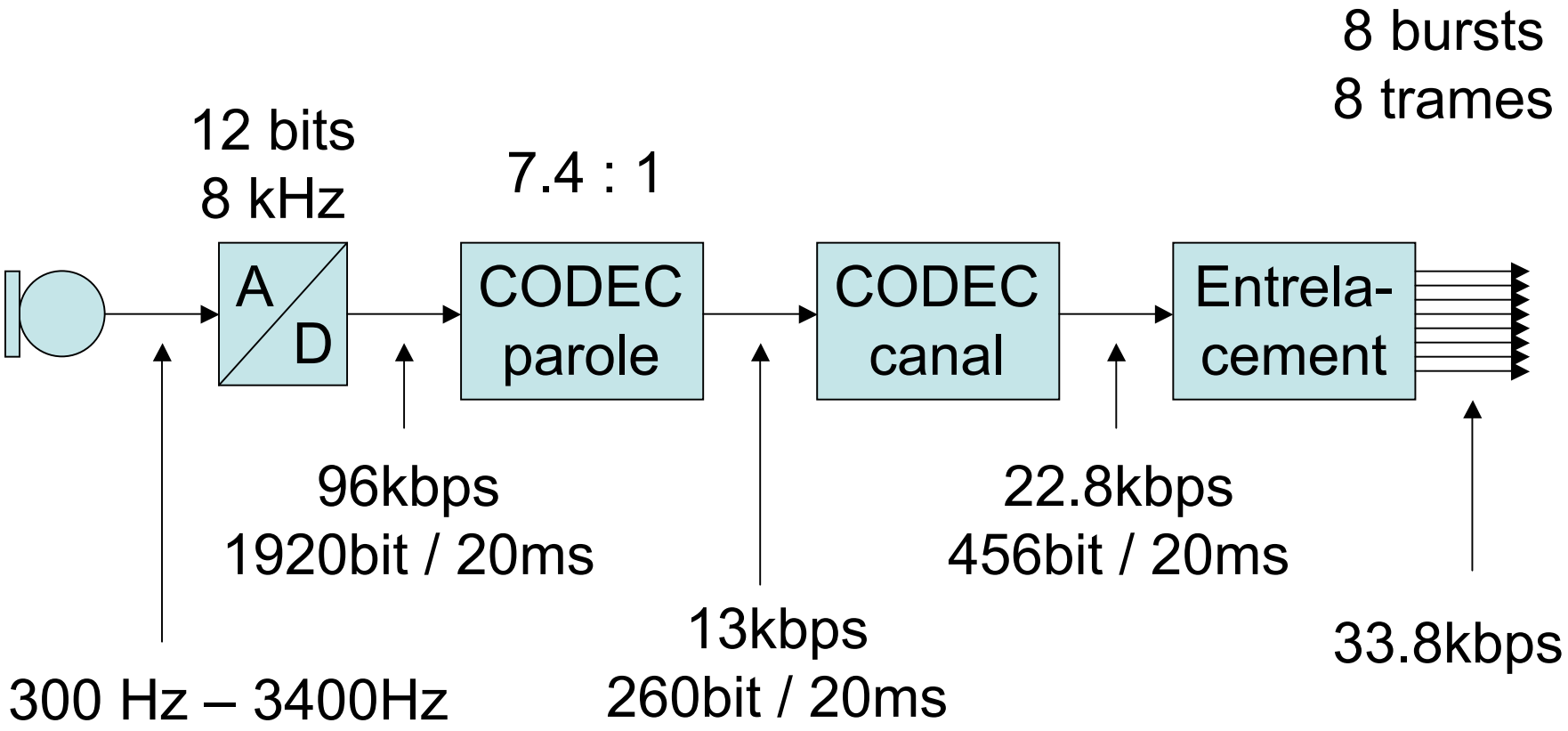
Codage de la parole

- 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).

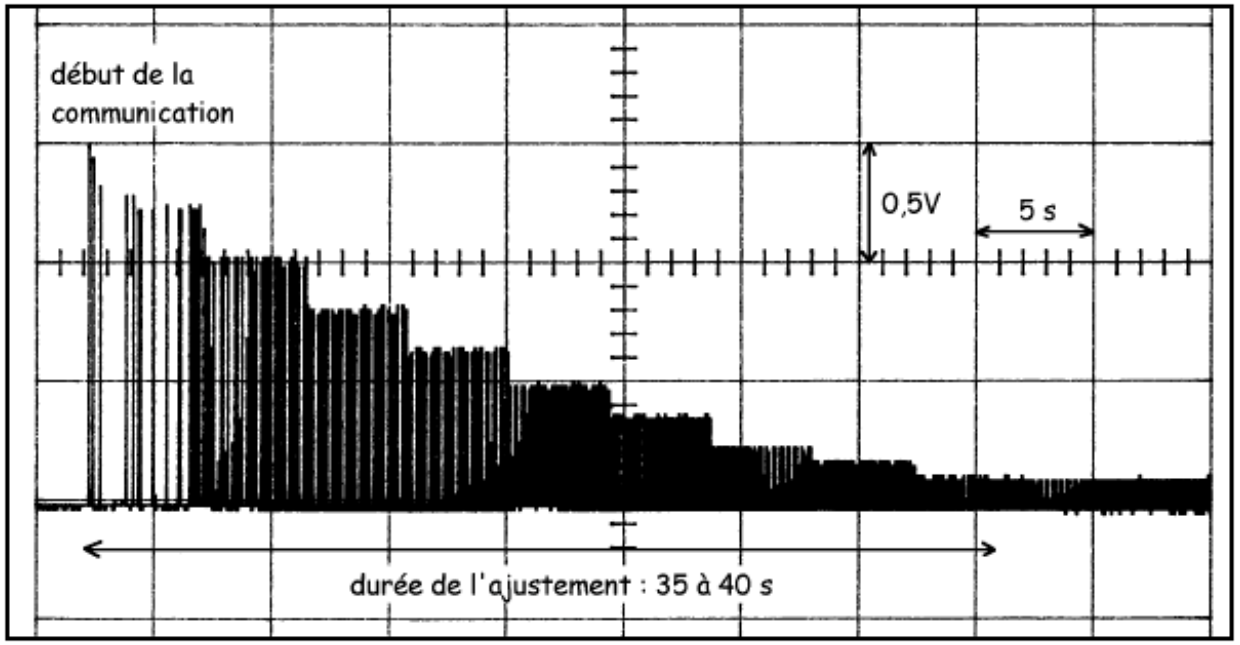
Codage de la parole



A/D : convertisseur Analogique -> Digital

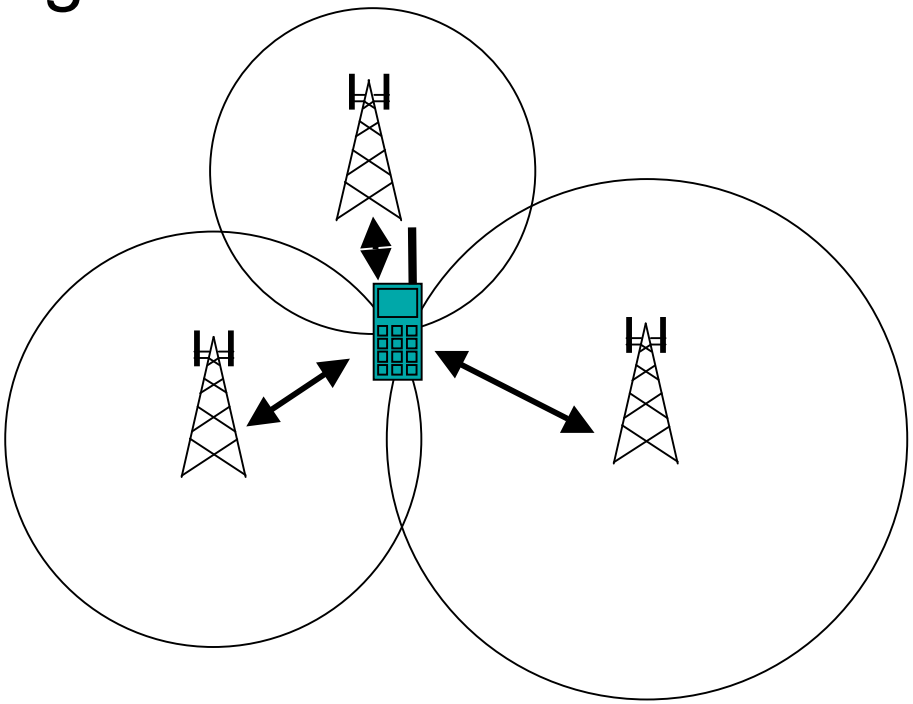
Contrôle de puissance d'émission

- 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



Positionnement, localisation

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



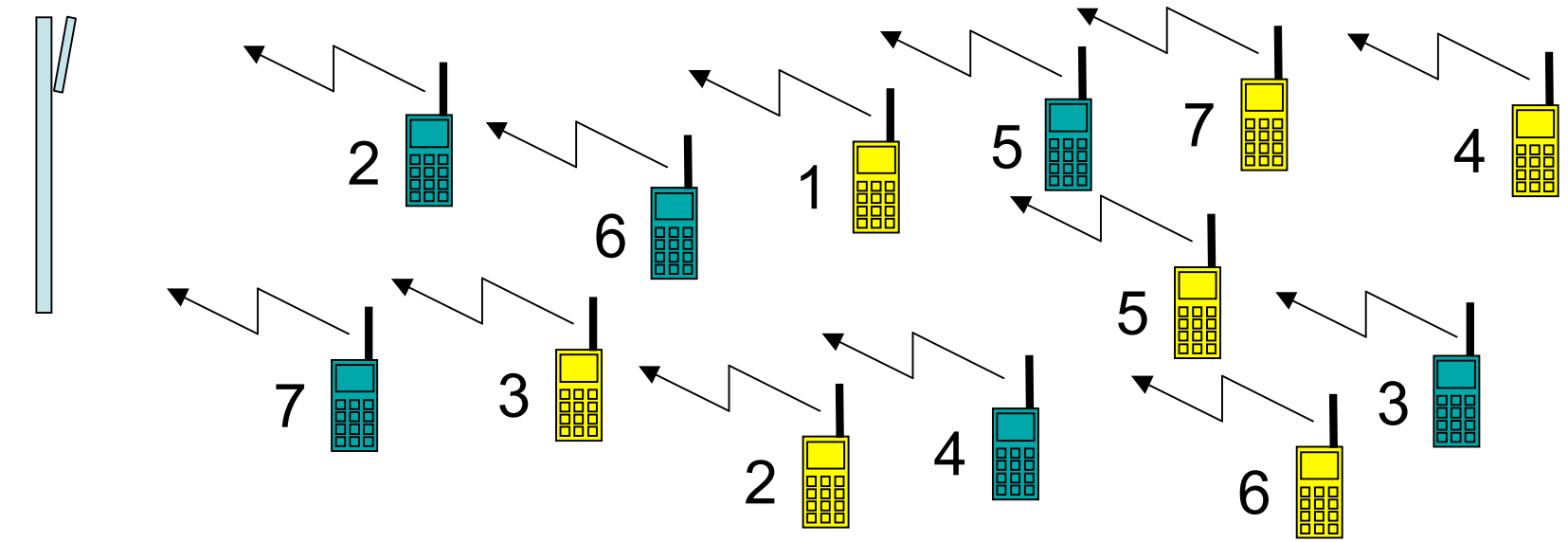
Changement de cellule

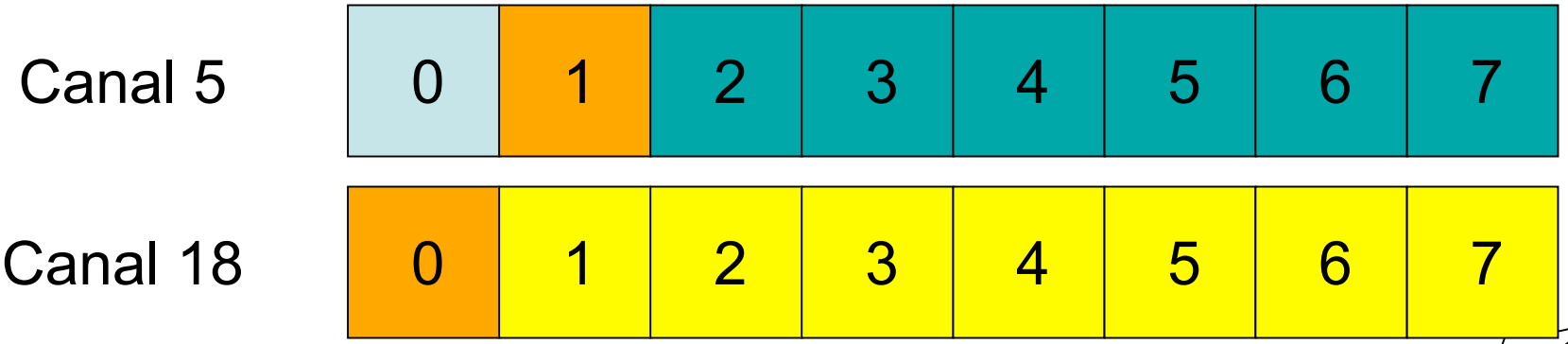
- Lors d'une conversation, le mobile écoute les BCH des cellules voisines. L'écoute se fait entre l'émission et la réception du *burst* suivant : mesure de niveau (peu de temps)
- Pour décoder les informations, le mobile s'arrête d'émettre et de recevoir toutes les 26 trames (slot *idle*): le mobile 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…

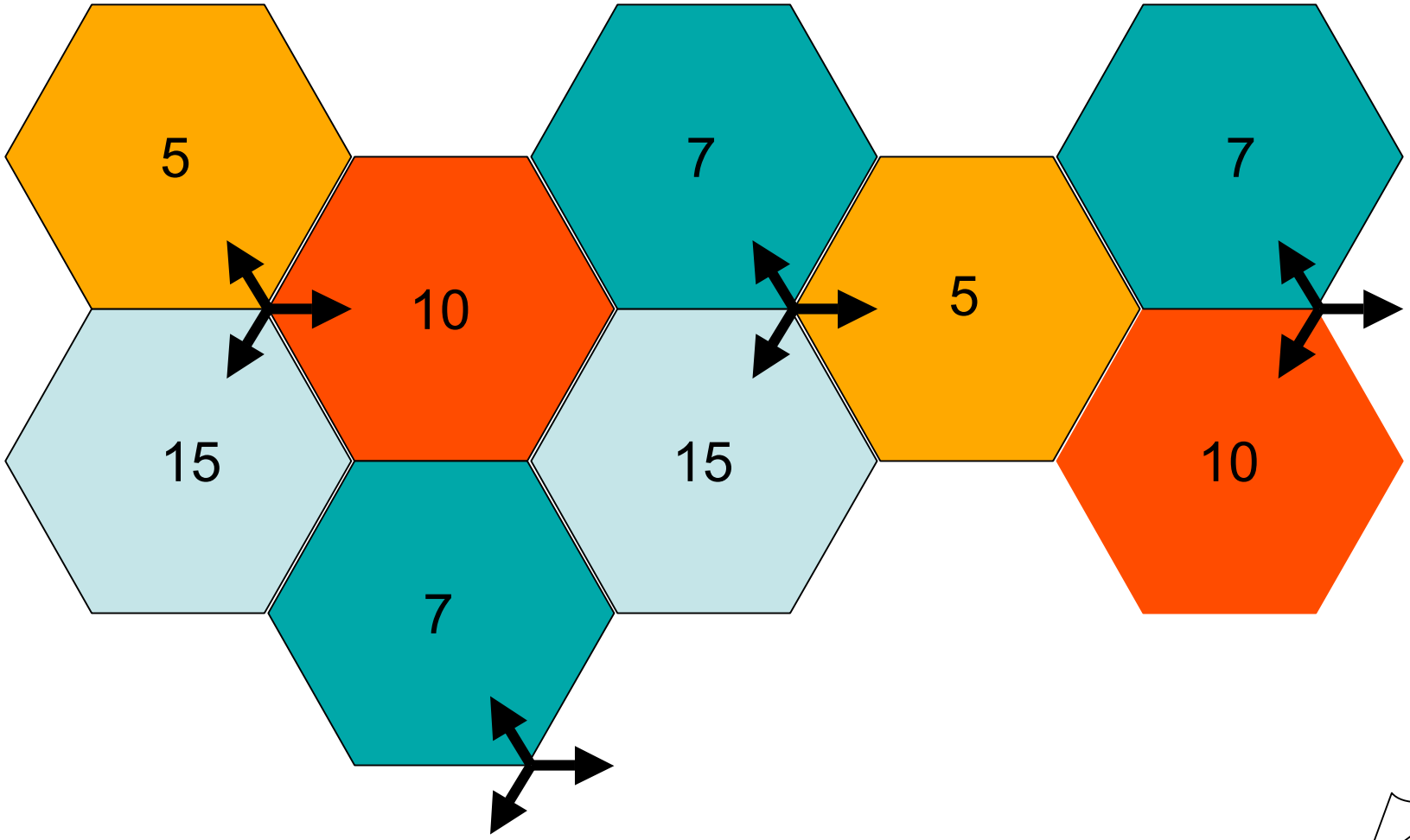
  26+26-51

Trafic / Capacité (2/2)





Réutilisation des fréquences



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

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)

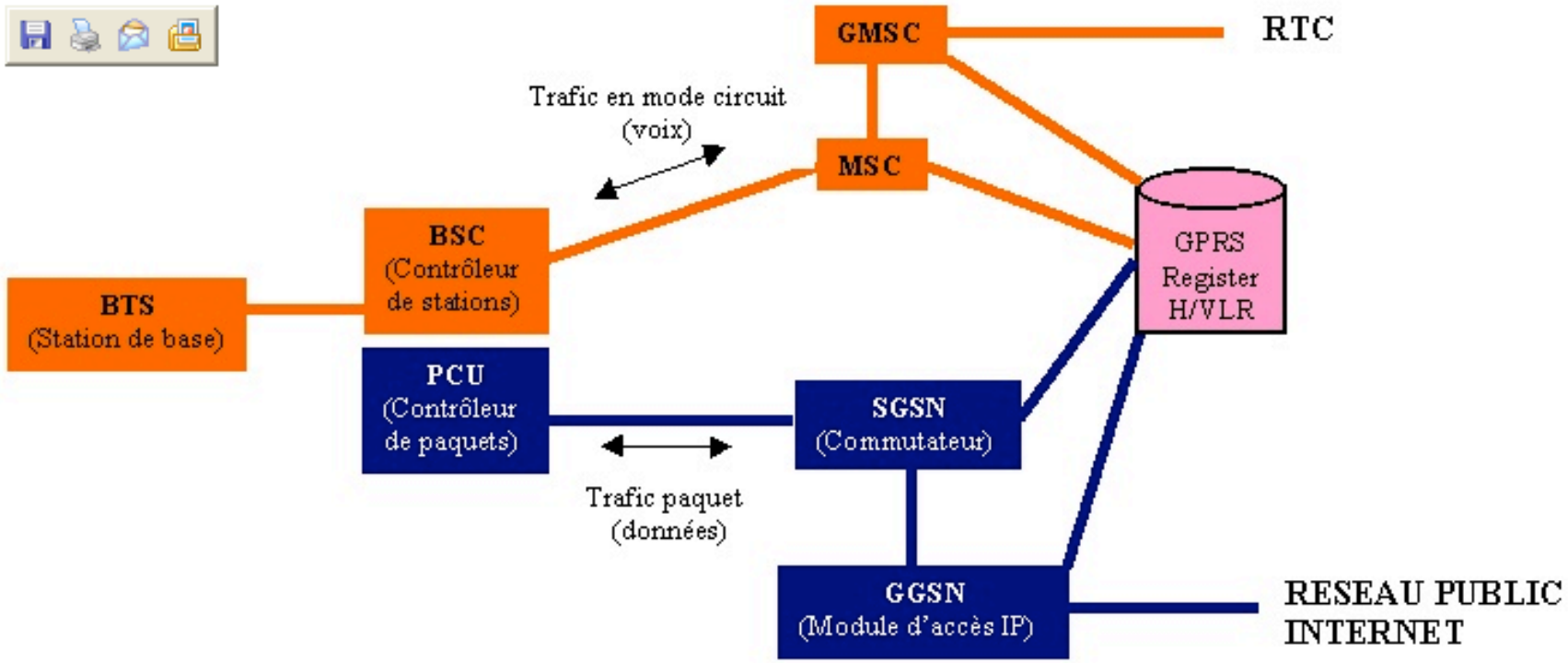
Codage de canal	Débit Utile	Protection
CS-1	9,05 kbit/s	++
CS-2	13,4 kbit/s	+
CS-3	15,6 kbit/s	-
CS-4	21,4 kbit/s	-- (aucune protection)

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.

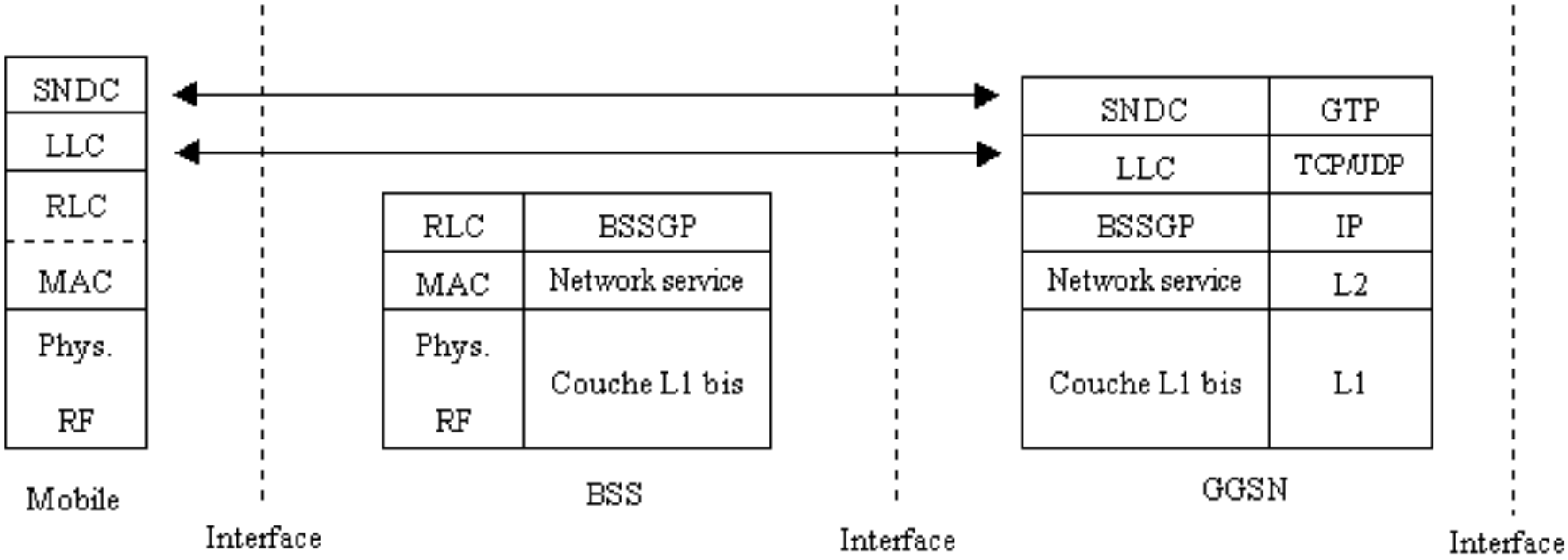
GPRS : structure du réseau



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 : couches logicielles



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

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

- 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

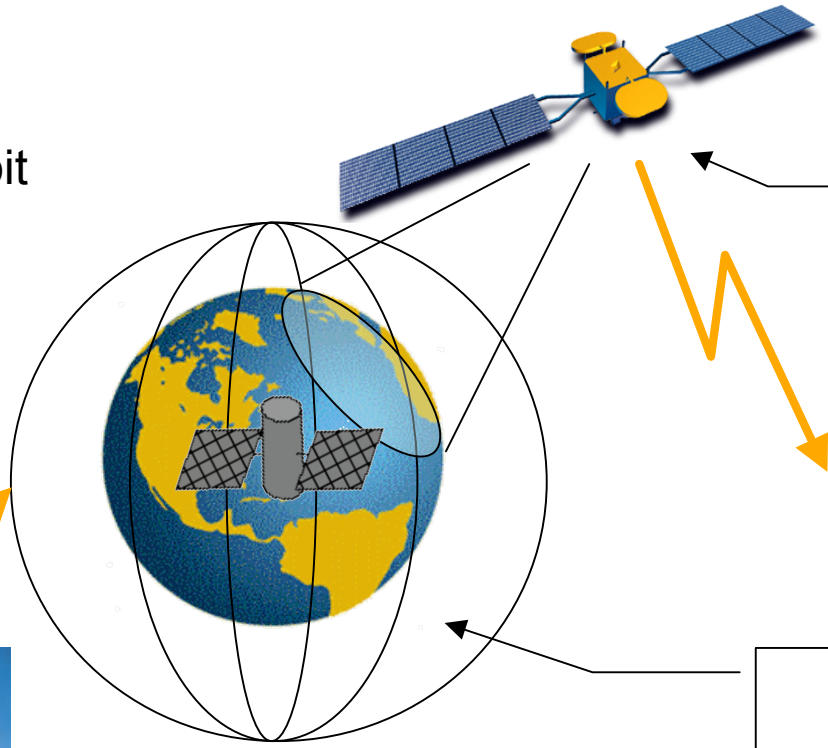
- La 3ème génération de téléphonie mobile est l'UMTS (Universal Mobile Telecommunication System).
- Cette nouvelle norme repose sur les technologies W-CDMA (combinaison de CDMA et FDMA) et TD-CDMA (combinaison de TDMA, CDMA et FDMA).
- Le principe de transmission repose sur l'étalement de spectre et 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

Orbite moyenne
MEO =
Medium Earth Orbit
~ 10000 kms



Satellite
géostationnaire
GEO
36000 kms

Orbite basse
LEO =
Low Earth Orbit
qq 100 kms

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

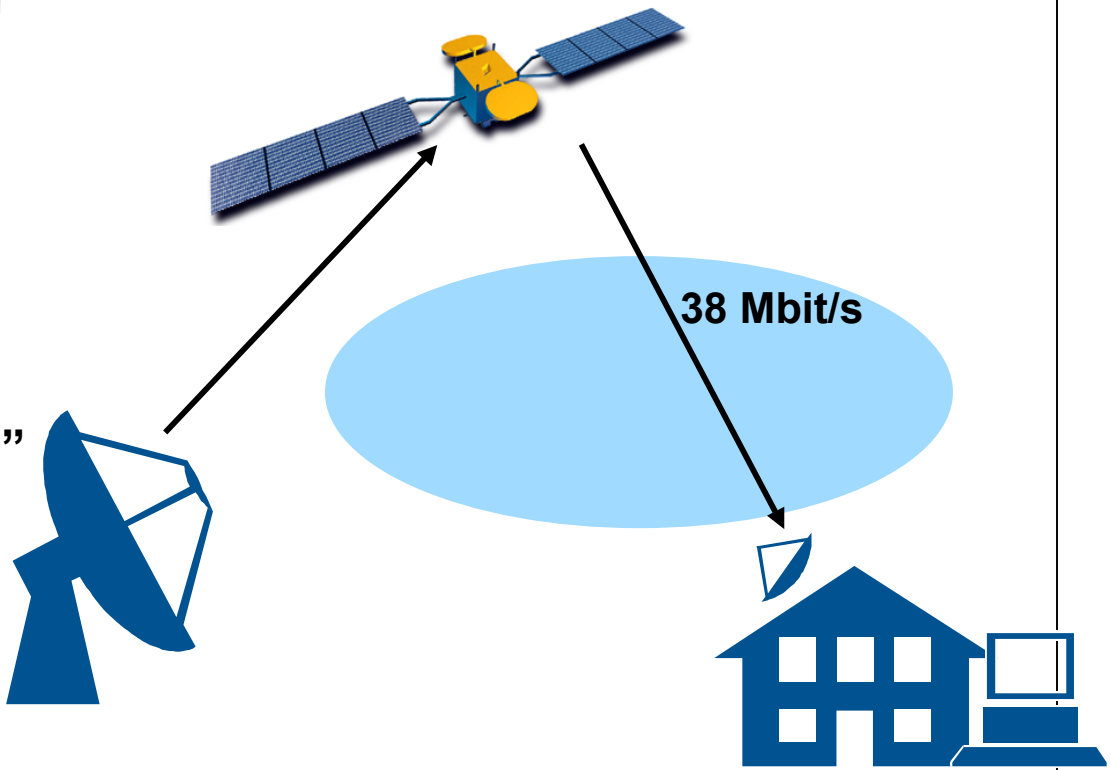
- Orbite : 10000 Kms
- Délai (A/R) : 80 ms
- Applications : voix (mobiles), data bas débit
- Débit : 300b/s à 38.4 kb/s
- Exemples : Odyssey, Ellipso

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 ...

Services à large bande par satellite

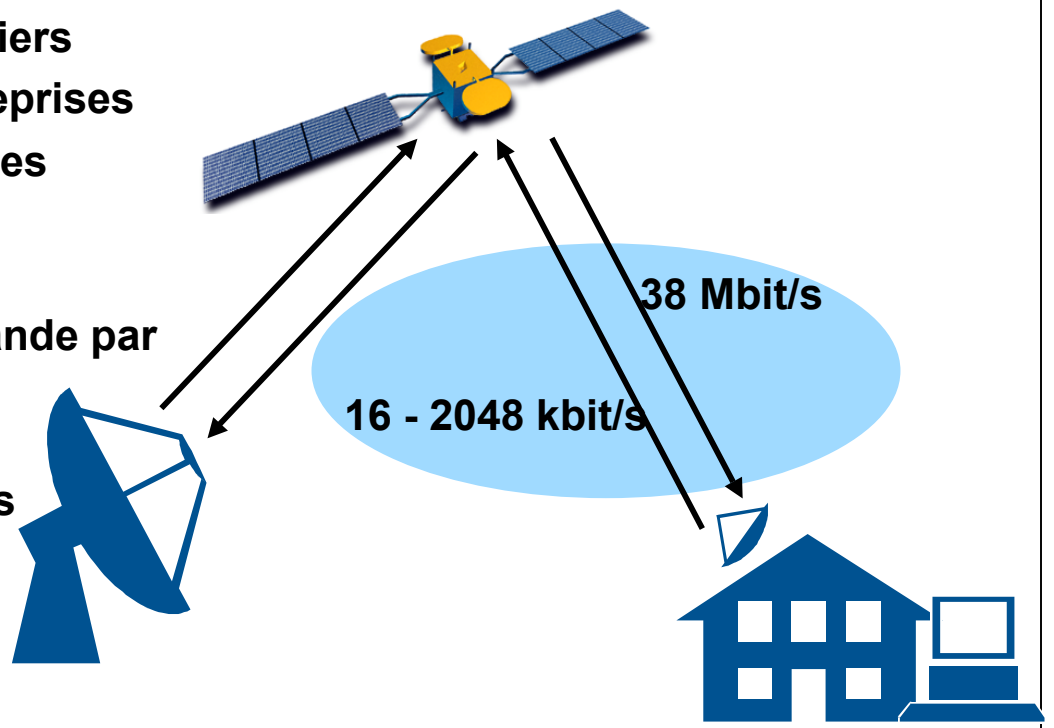
- **Distribution de services à voie unique avec voie de retour terrestre**
  - **Services**
    - **A-DSL par satellite pour particuliers**
    - **Services large bande pour entreprises**
  - **Services “co-positionnés” avec les transmissions TV**



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**



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

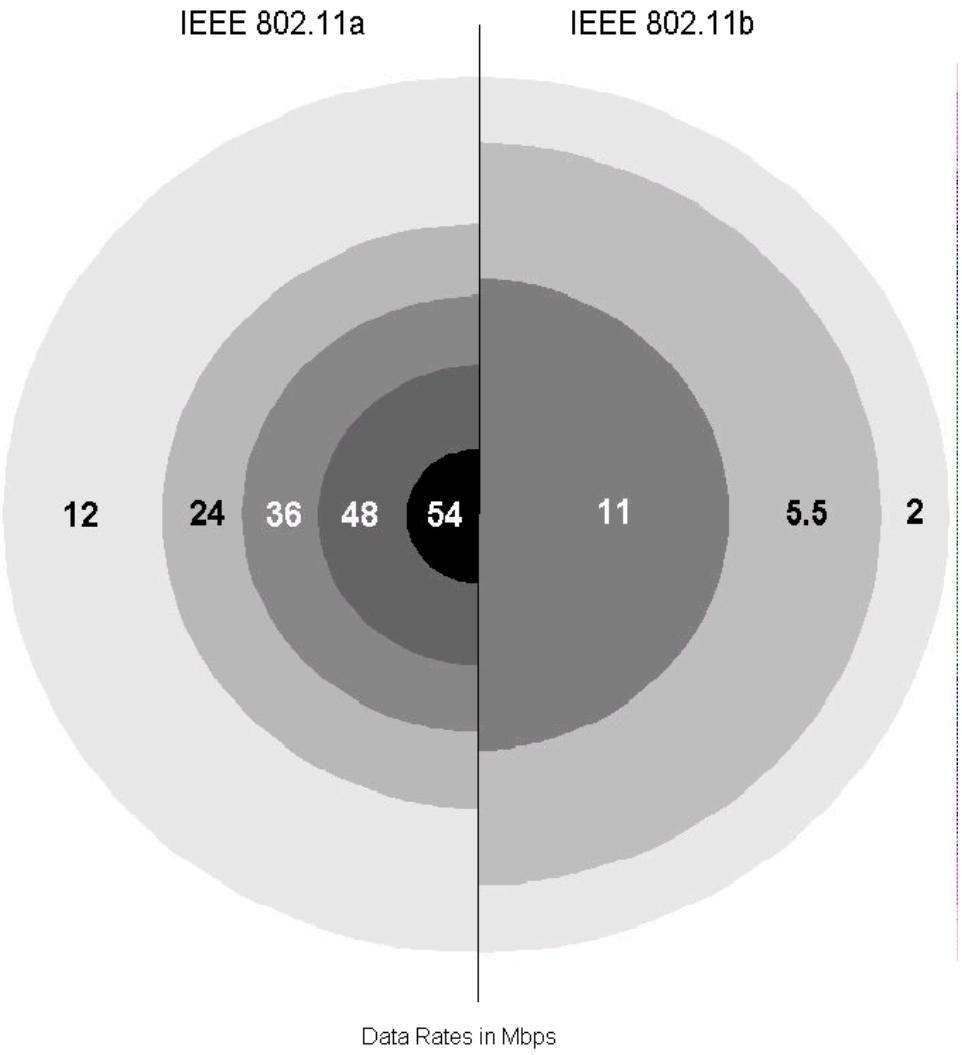
Standards IEEE 802.11

- **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.

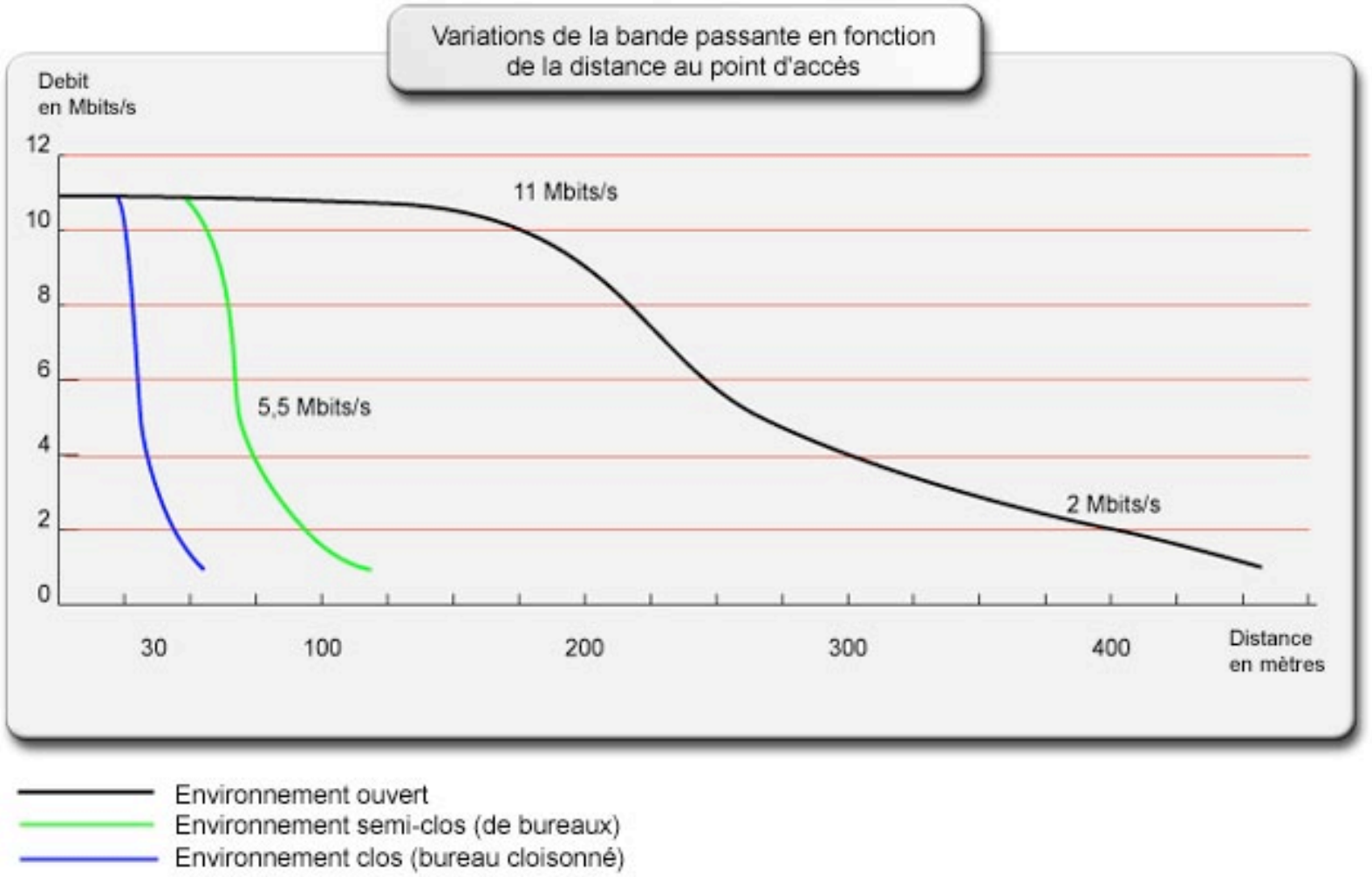
Standards les plus courants IEEE 802.11

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.

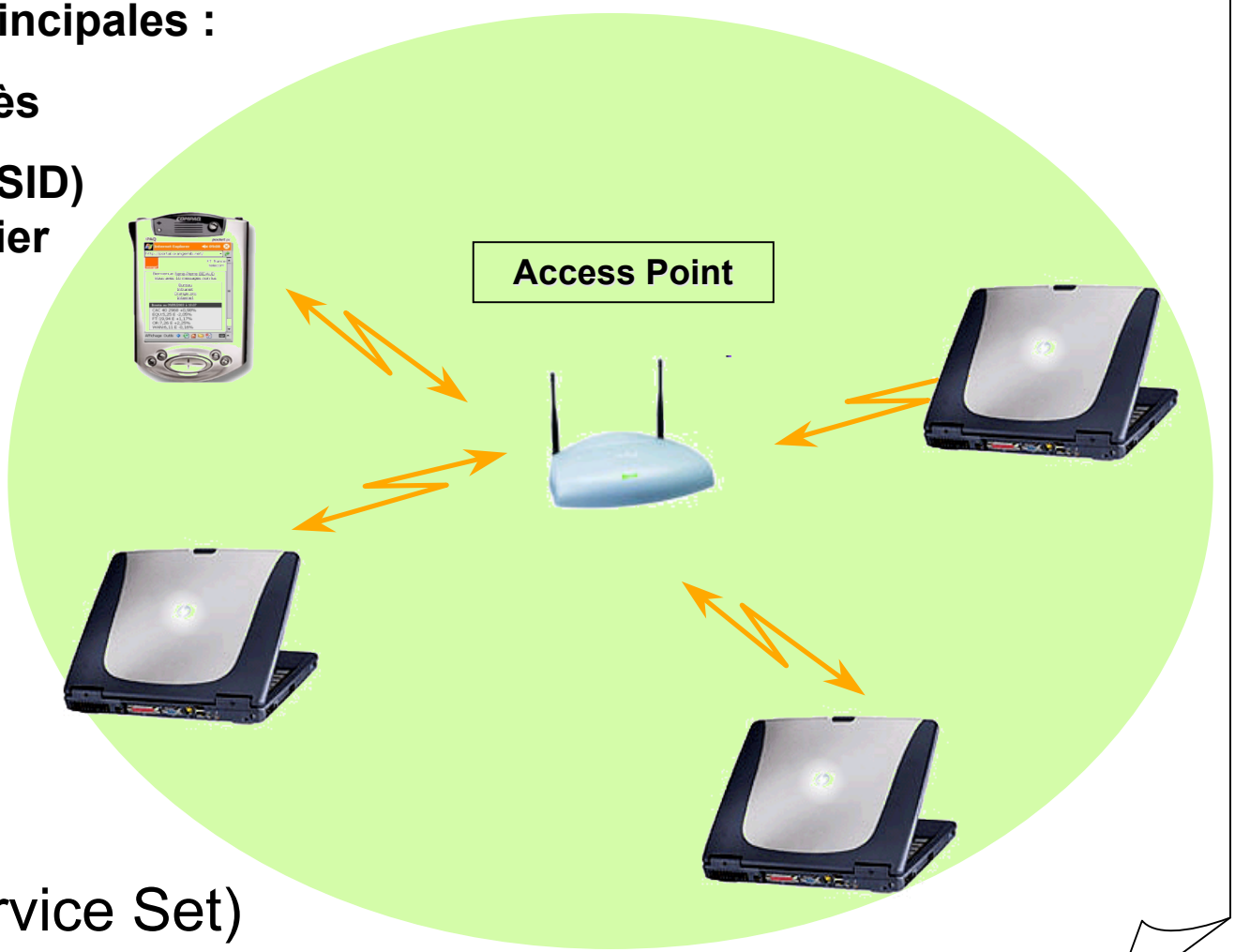
IEEE 802.11 : Architecture

- 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**



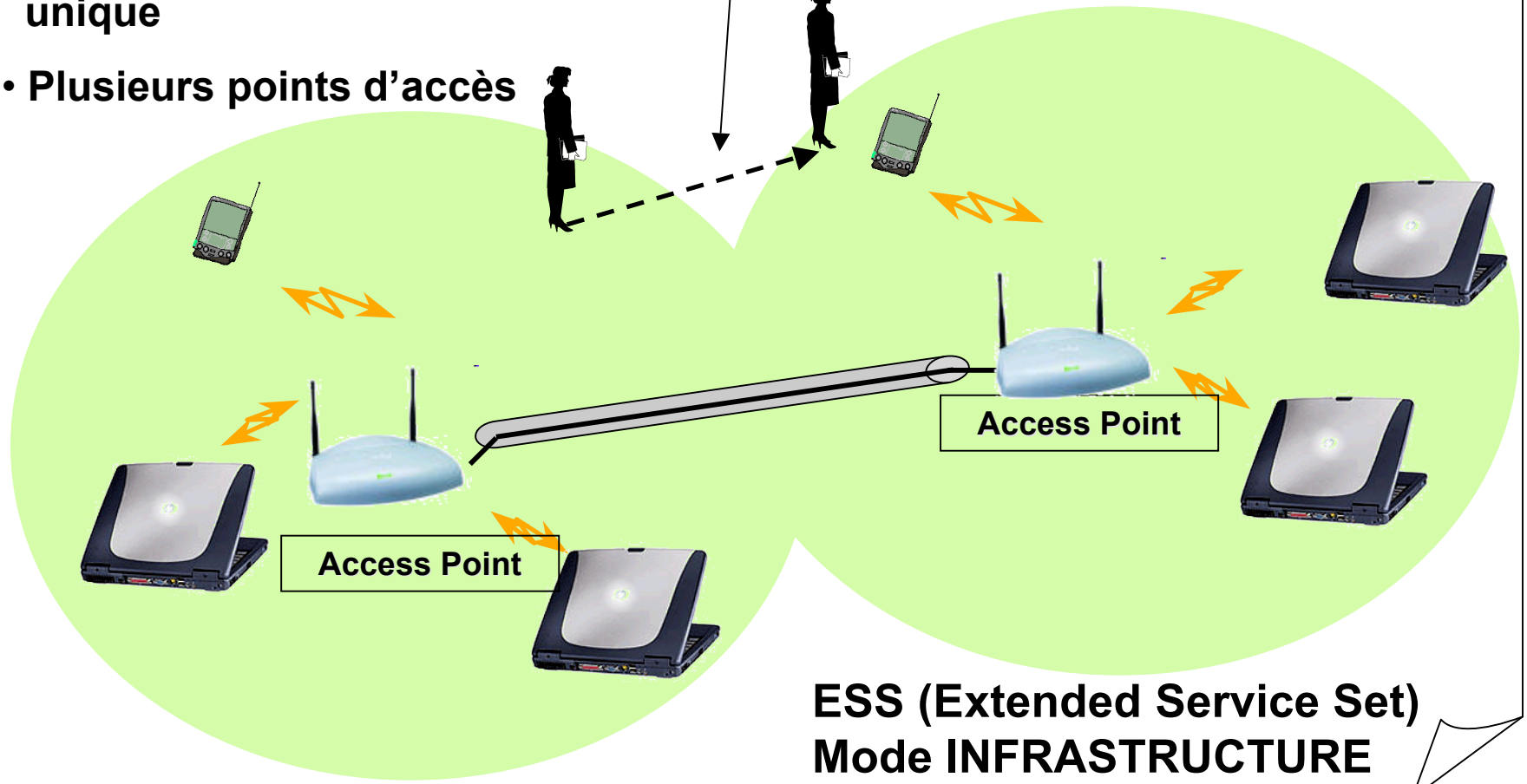
BSS (Basic Service Set)

IEEE 802.11 : Architecture ESS et handover

Caractéristiques principales :

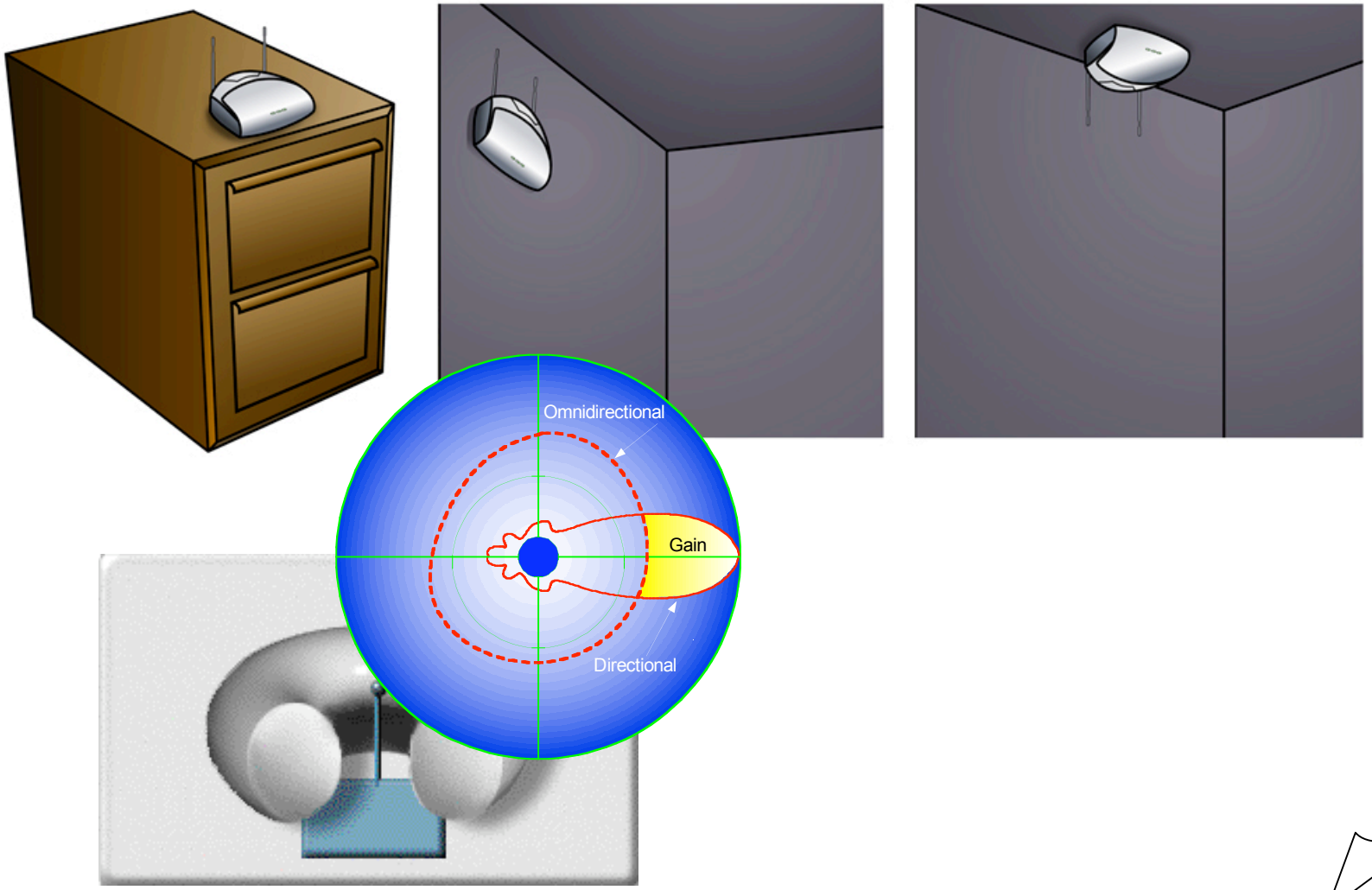
- **Nom de réseau (SSID) unique**
- **Plusieurs points d'accès**

Mécanisme de handover



ESS (Extended Service Set)
Mode INFRASTRUCTURE

Antennes : orientation



IEEE 802.11

Couche physique

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

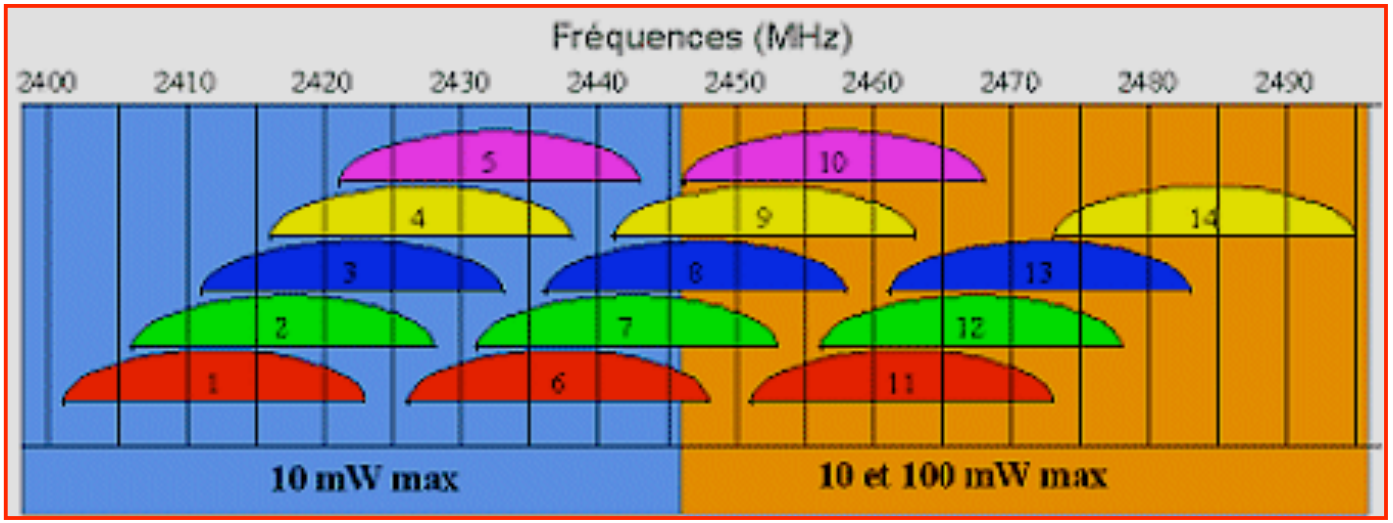
Types de modulation

- 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)

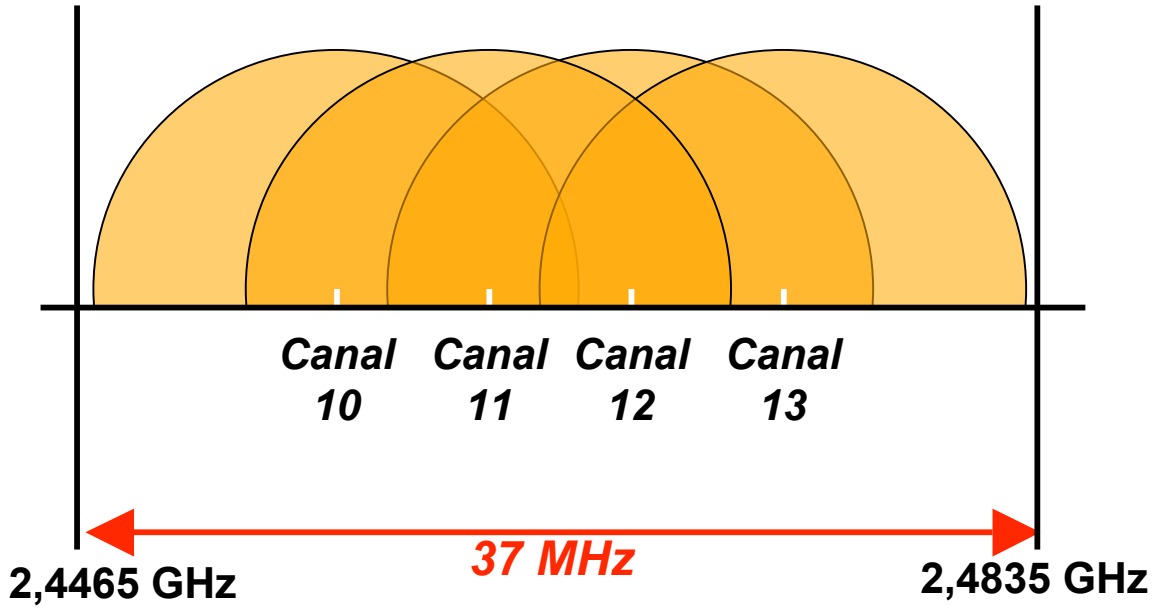
- Bande ISM
  - Bande divisée en 14 canaux de 20 MHz
  - Problème de recouvrement
  - Superposition de 3 réseaux au sein d'un même espace
  - Largeur de bande 83 MHZ



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



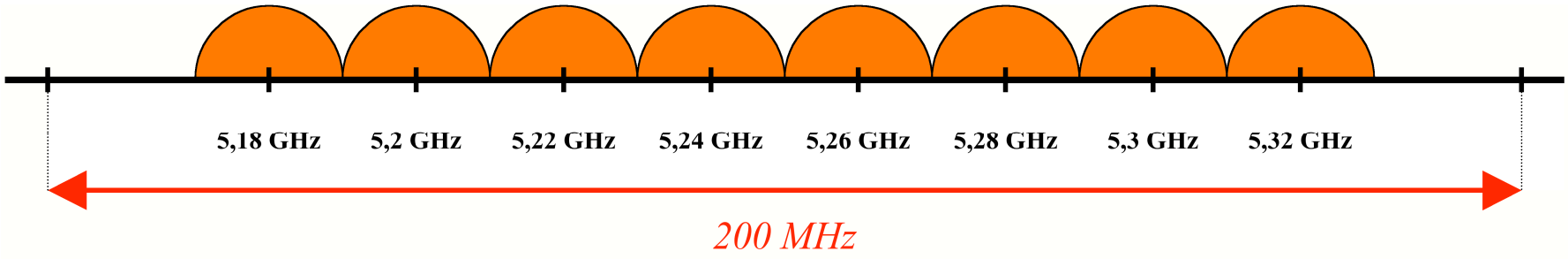
802.11b - Portée

- 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

<table>
<tr><td rowspan="2">Couche liaison
de données</td><td>LLC 802.2
Contrôle de liaison logique</td></tr>
<tr><td>MAC 802.11, sécurité, etc …
Contrôle d'accès au support</td></tr>
</table>

- 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

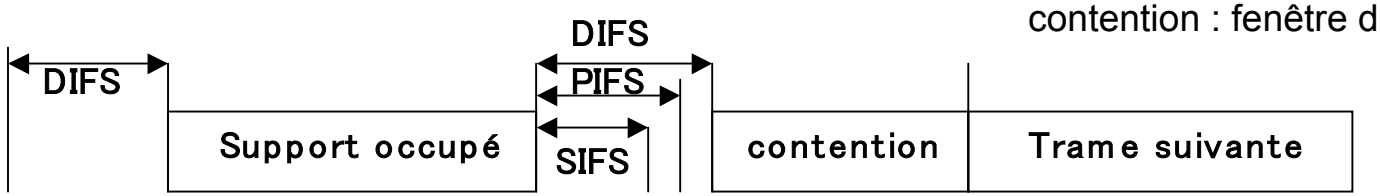
Méthode d'accès

- **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



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 …)

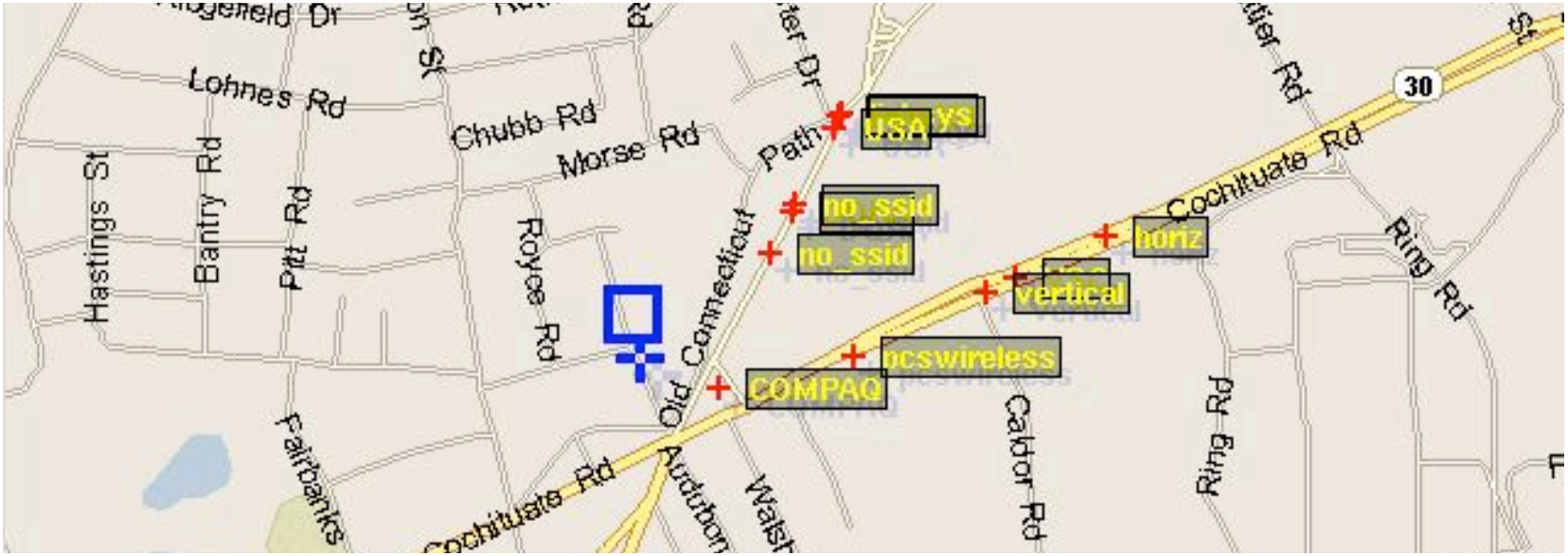
Les attaques : refus de service

- **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

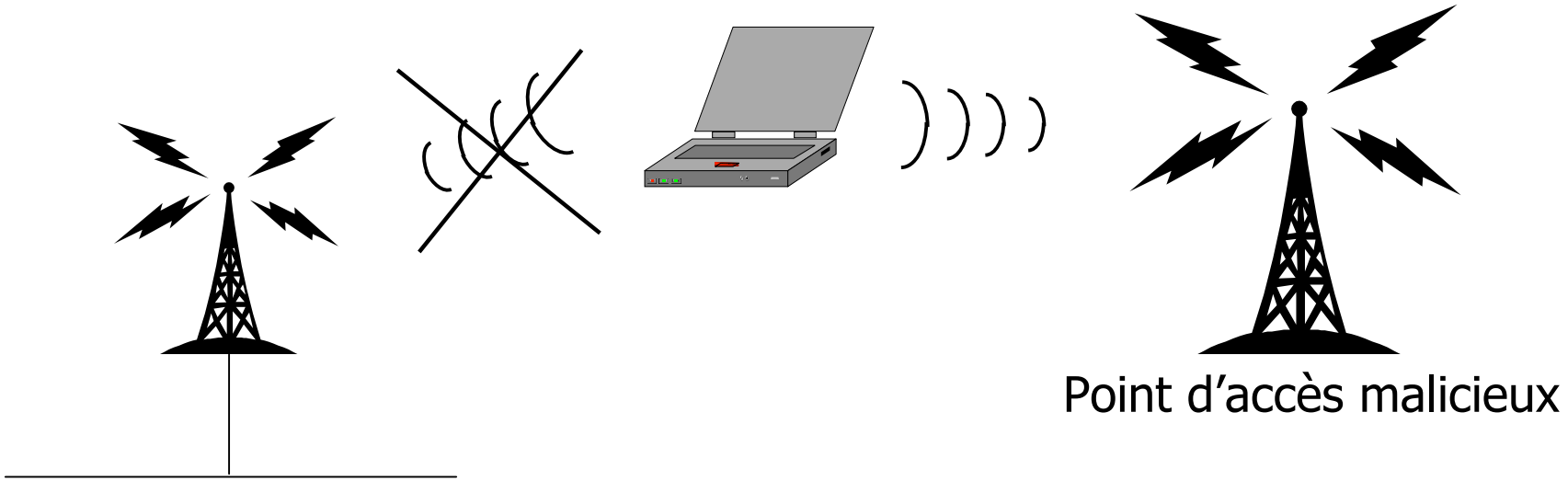
Un jeu : le **War Driving** = Quadrillage d'une ville avec

- ✓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

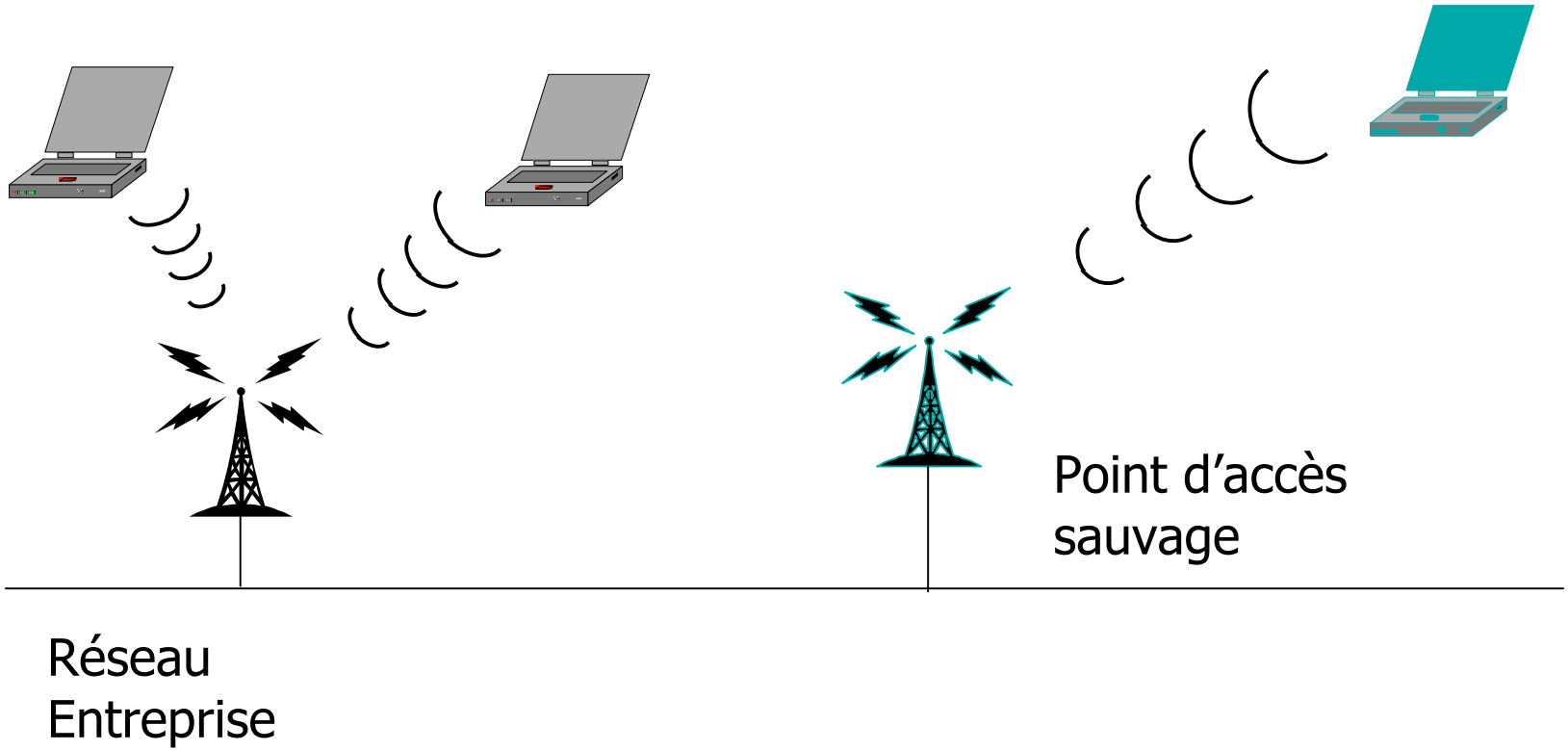
- Point d'accès «malicieux»



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

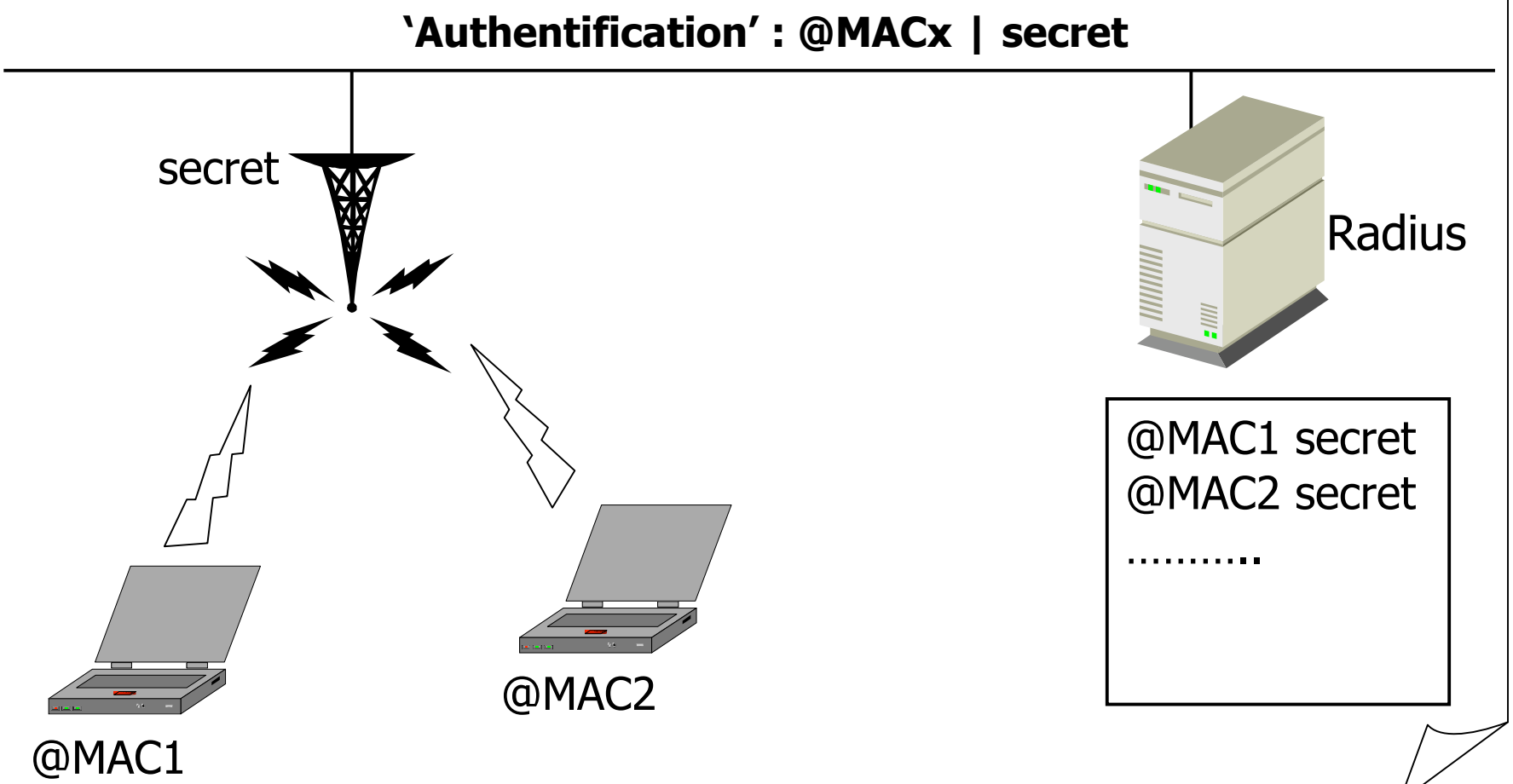
- N’autoriser que certaines adresses à se connecter aux points d’accès.

- 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"

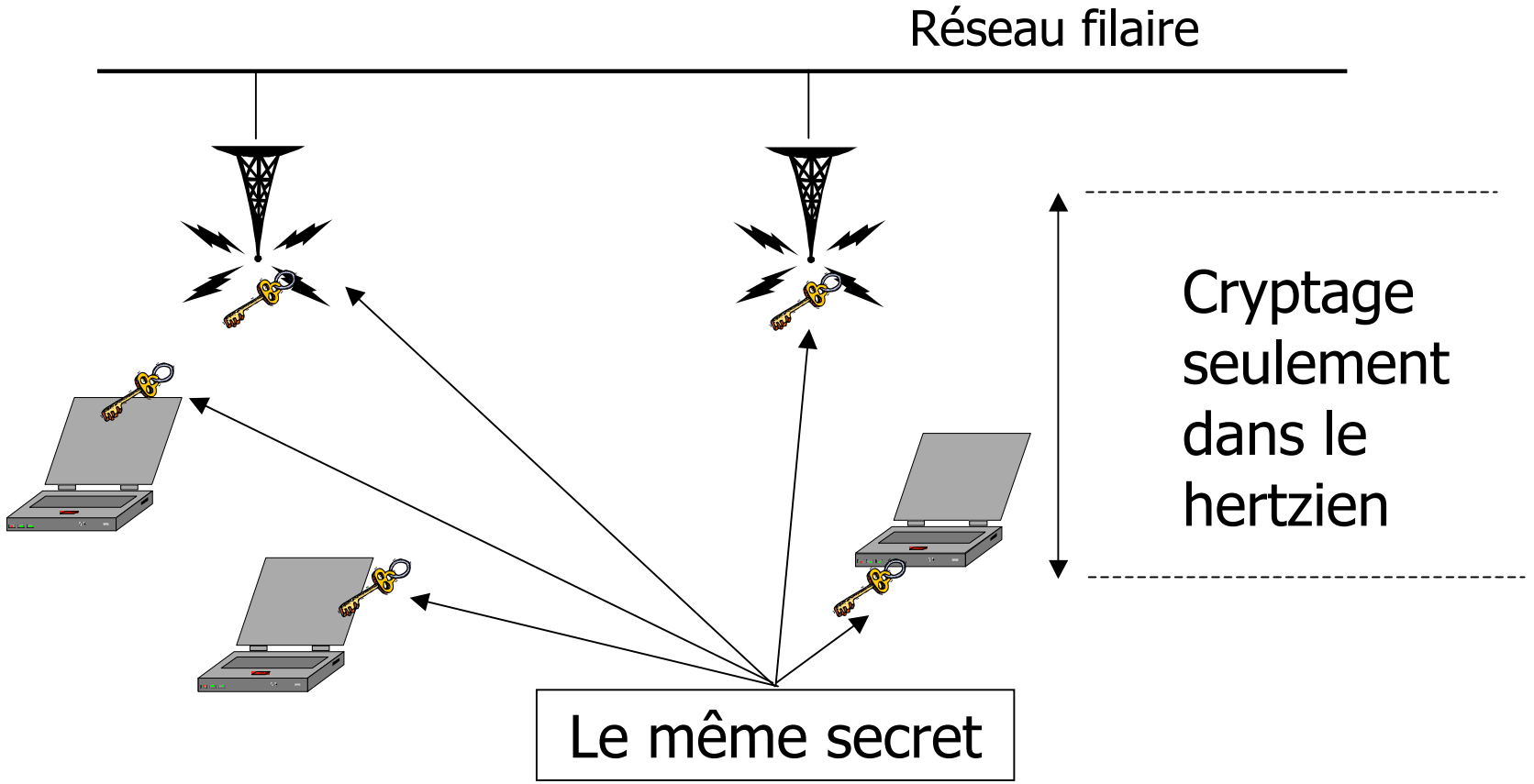
Wired Equivalent Privacy

- 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.

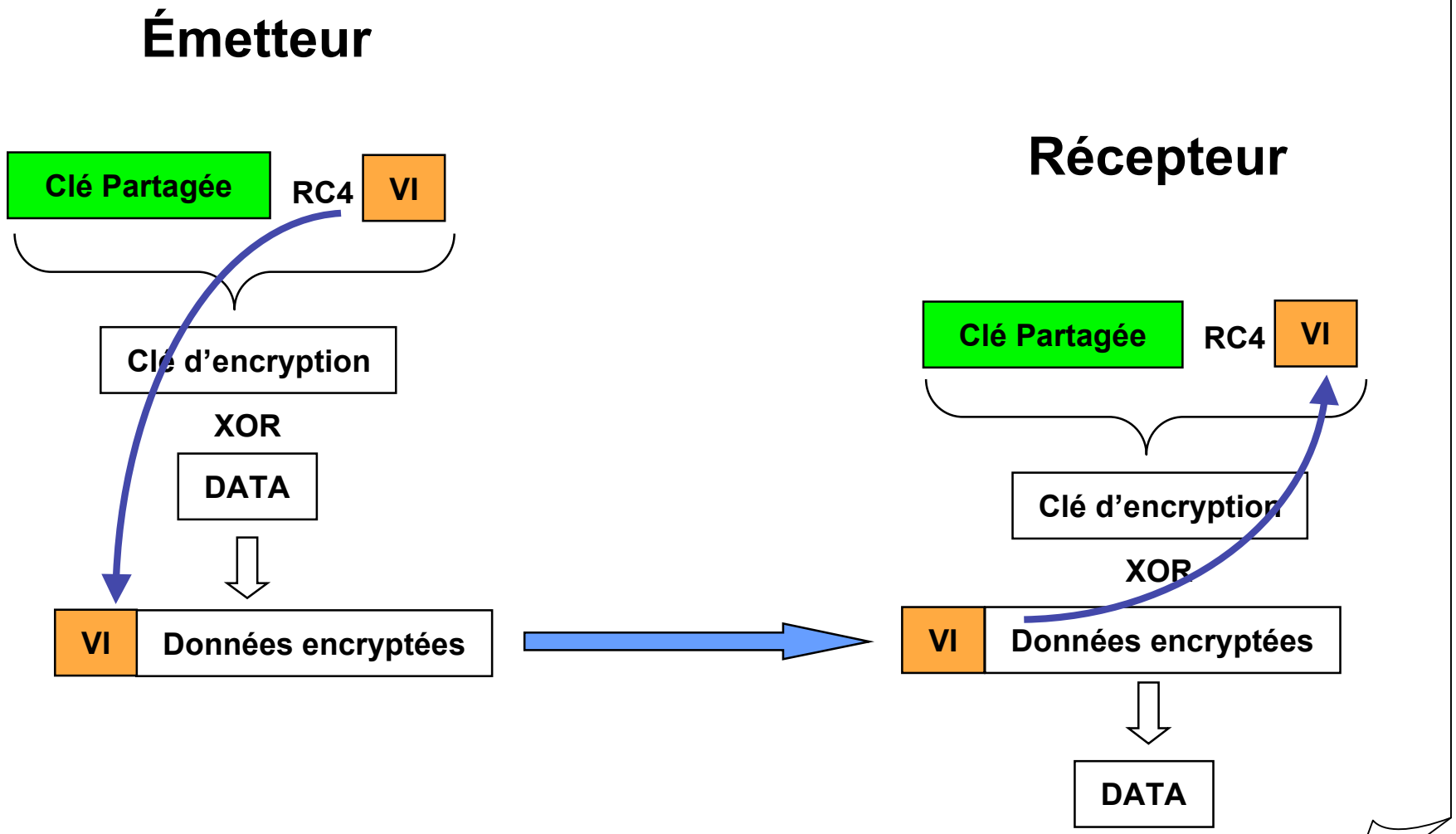
Wired Equivalent Privacy



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



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