Réseaux sans-fil

Florent Dupont

fdupont@liris.cnrs.fr

https://perso.liris.cnrs.fr/florent.dupont/Enseignement/RSFM/Reseaux-sans-fil.pdf

https://perso.liris.cnrs.fr/florent.dupont/Enseignement/RSFM/RSFM.html

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
  - les problèmes de sécurité
  - etc.

➢ Enjeu économique et social

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)

- ***ARCEP – Autorité de Régulation des Télécommunications*** *http://www.art-telecom.fr/*

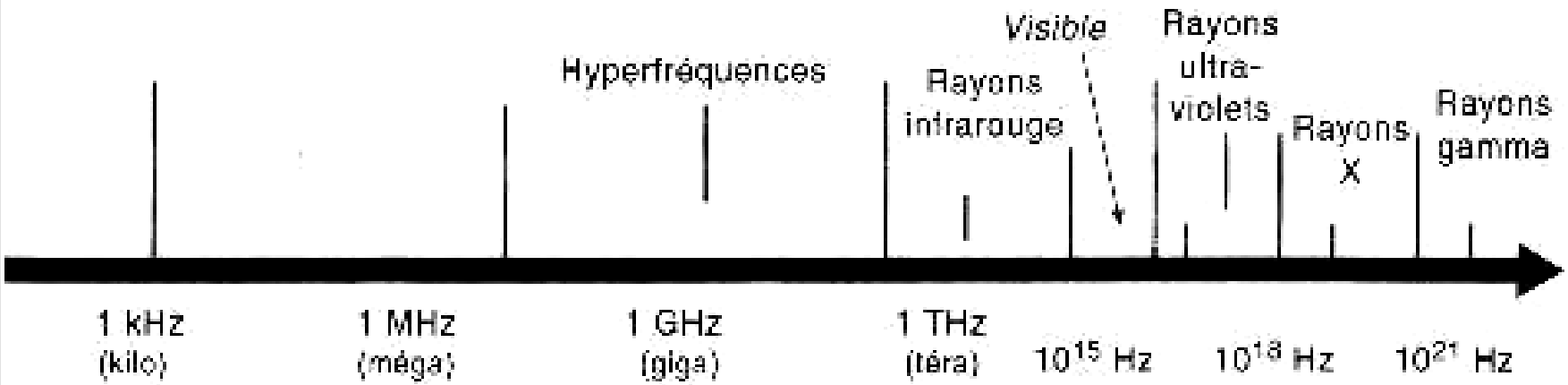
+ nombreux sites…

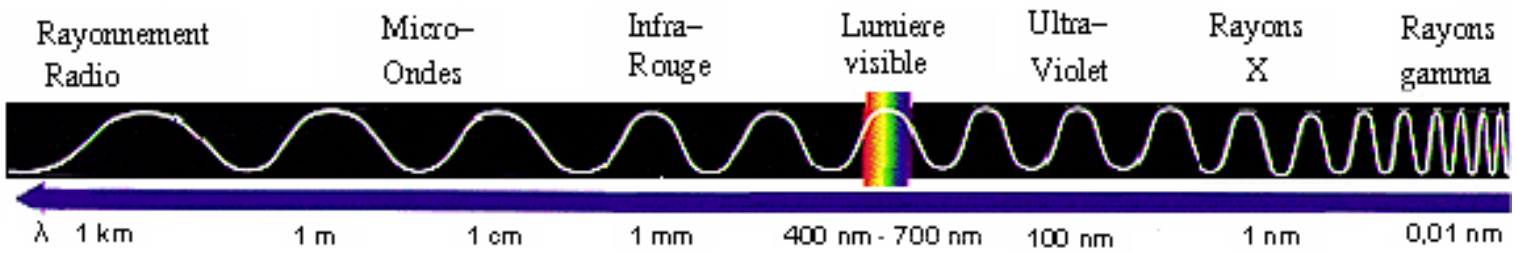
Plan du cours

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

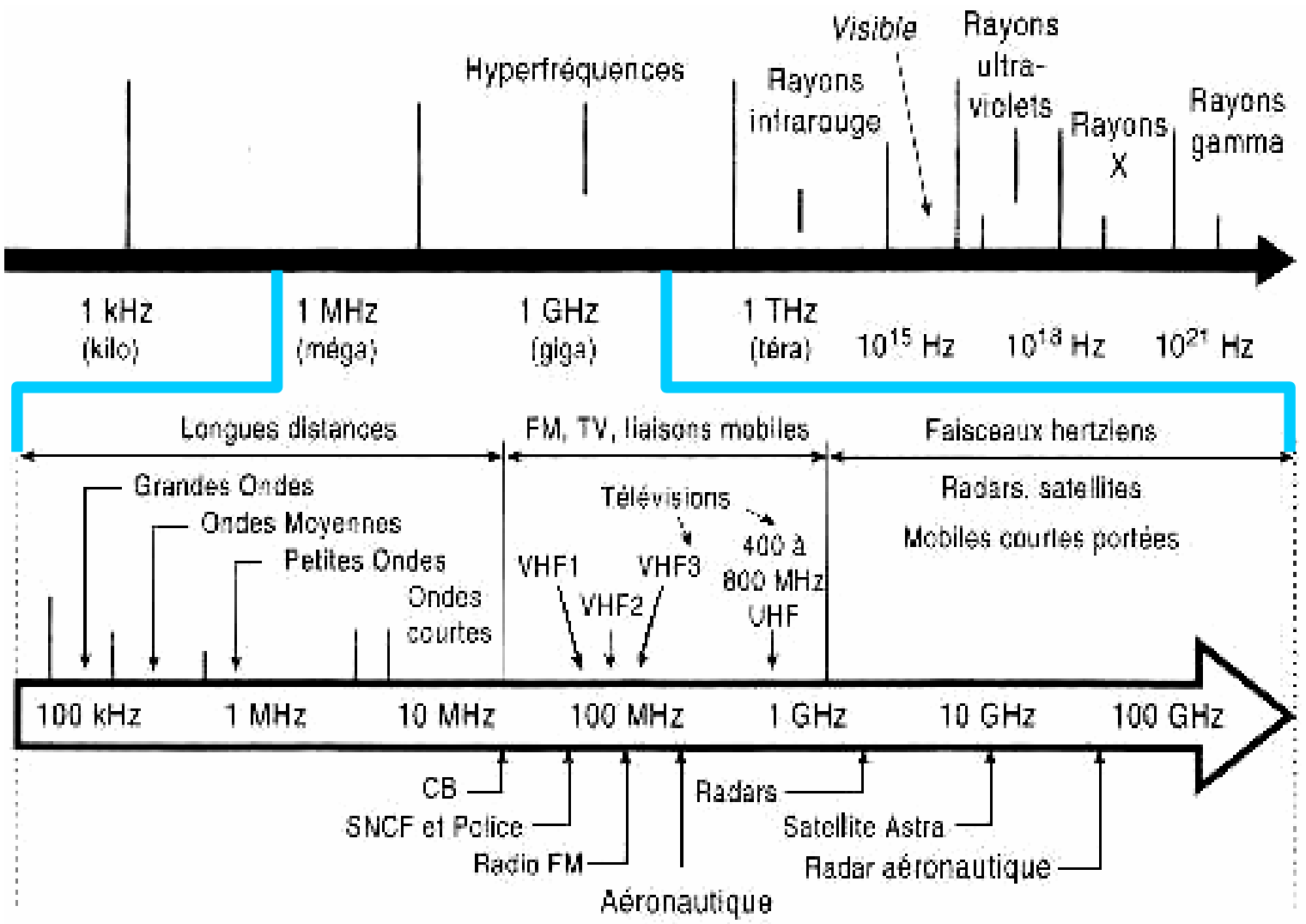
Utilisation des bandes de fréquences

Utilisation des bandes de fréquences





Utilisation des bandes de fréquences



Agence nationale des fréquences (www.anfr.fr)

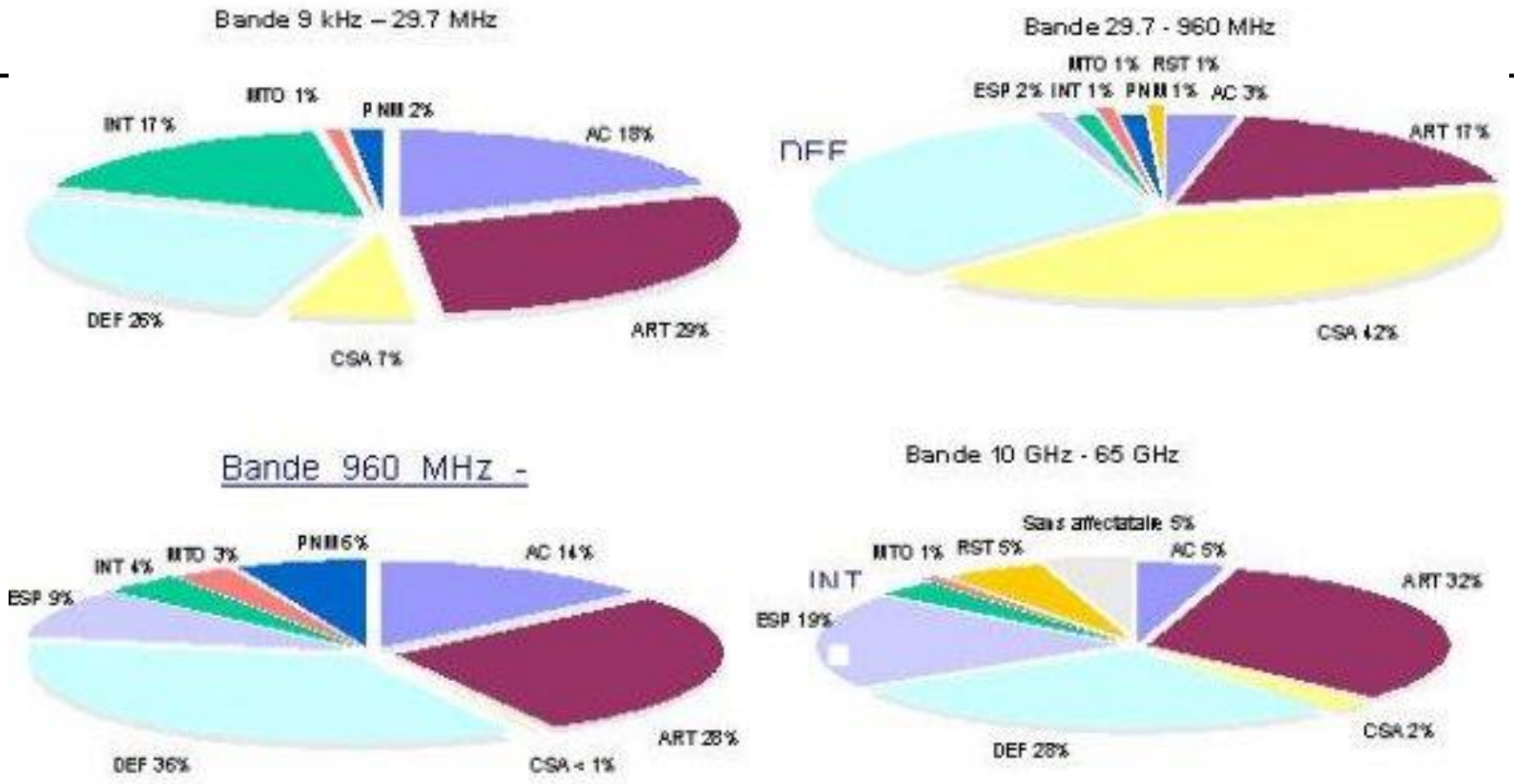
- **Bandes de fréquences** : attribuées aux différents services de radiocommunication par le ***Règlement des radiocommunications*** de **l'Union internationale des télécommunications**, élaboré par les conférences mondiales des radiocommunications.
- **En France, les bandes ainsi attribuées sont réparties 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.anfr.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

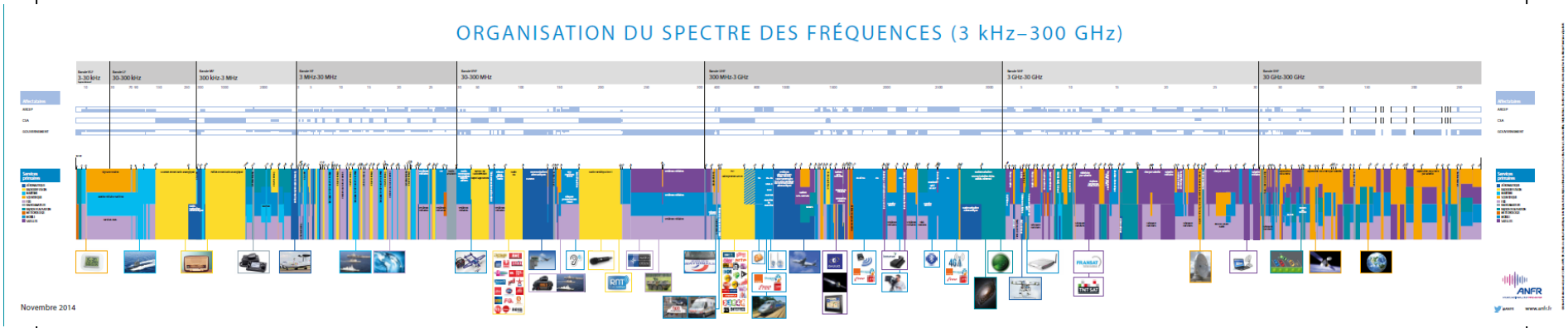


- Aviation civile (AC)
- Autorité de régulation des télécommunications (ART)
- Conseil supérieur de l'audiovisuel (CSA)
- Ministère de la défense (DEF)
- Espace (ESP)
- Ministère de l'intérieur (INT)
- Météorologie (MTO)
- Ports et navigation maritime (PNM)
- Radioastronomie (RST)

Répartition des bandes de fréquence

- Frise interactive disponible (site anfr) :

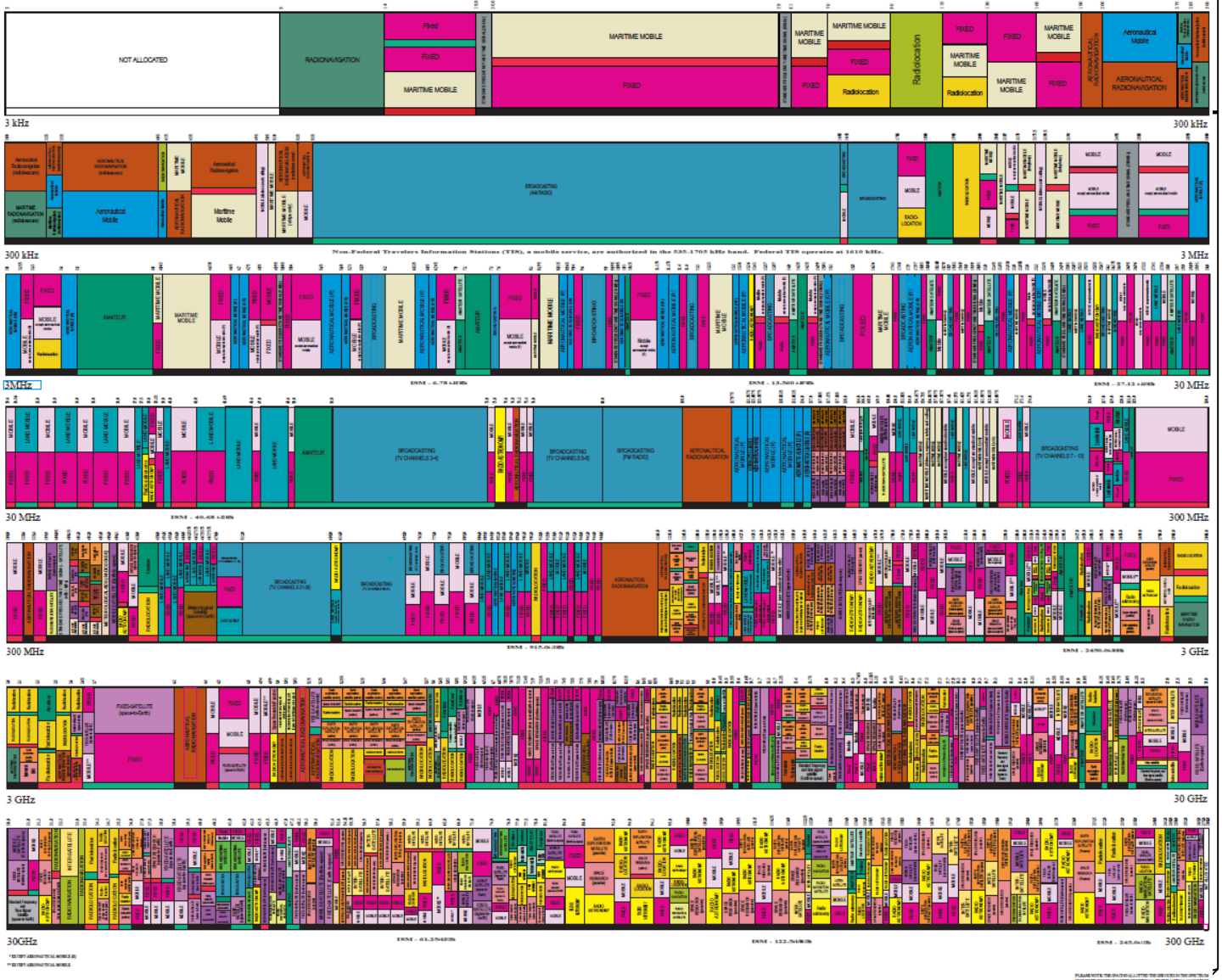
http://www.anfr.fr/gestion-des-frequences-sites/tnrbf/frise-interactive/#menu2



https://www.cartoradio.fr/#/cartographie/all/lonlat/4.864823/45.778922

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM



RADIO SERVICES COLOR LEGEND

AERONAUTICAL MOBILE
AERONAUTICAL MOBILE SATELLITE
AERONAUTICAL RADIONAVIGATION
AMATEUR
AMATEUR SATELLITE
BROADCASTING
BROADCASTING SATELLITE
EARTH EXPLORATION SATELLITE
FIXED
FIXED SATELLITE
INTER-SATELLITE
LAND MOBILE
LAND MOBILE SATELLITE
MARITIME MOBILE
MARITIME MOBILE SATELLITE
MARITIME RADIONAVIGATION
METEOROLOGICAL
METEOROLOGICAL SATELLITE
MOBILE
MOBILE SATELLITE
RADIO ASTRONOMY
RADIODETERMINATION SATELLITE
RADIOLOCATION
RADIOLOCATION SATELLITE
RADIONAVIGATION
RADIONAVIGATION SATELLITE
SPACE OPERATION
SPACE RESEARCH
STANDARD FREQUENCY AND TIME SIGNAL
STANDARD FREQUENCY AND TIME SIGNAL SATELLITE

ACTIVITY CODE

GOVERNMENT EXCLUSIVE
GOVERNMENT/NON-GOVERNMENT SHARED
NON-GOVERNMENT EXCLUSIVE

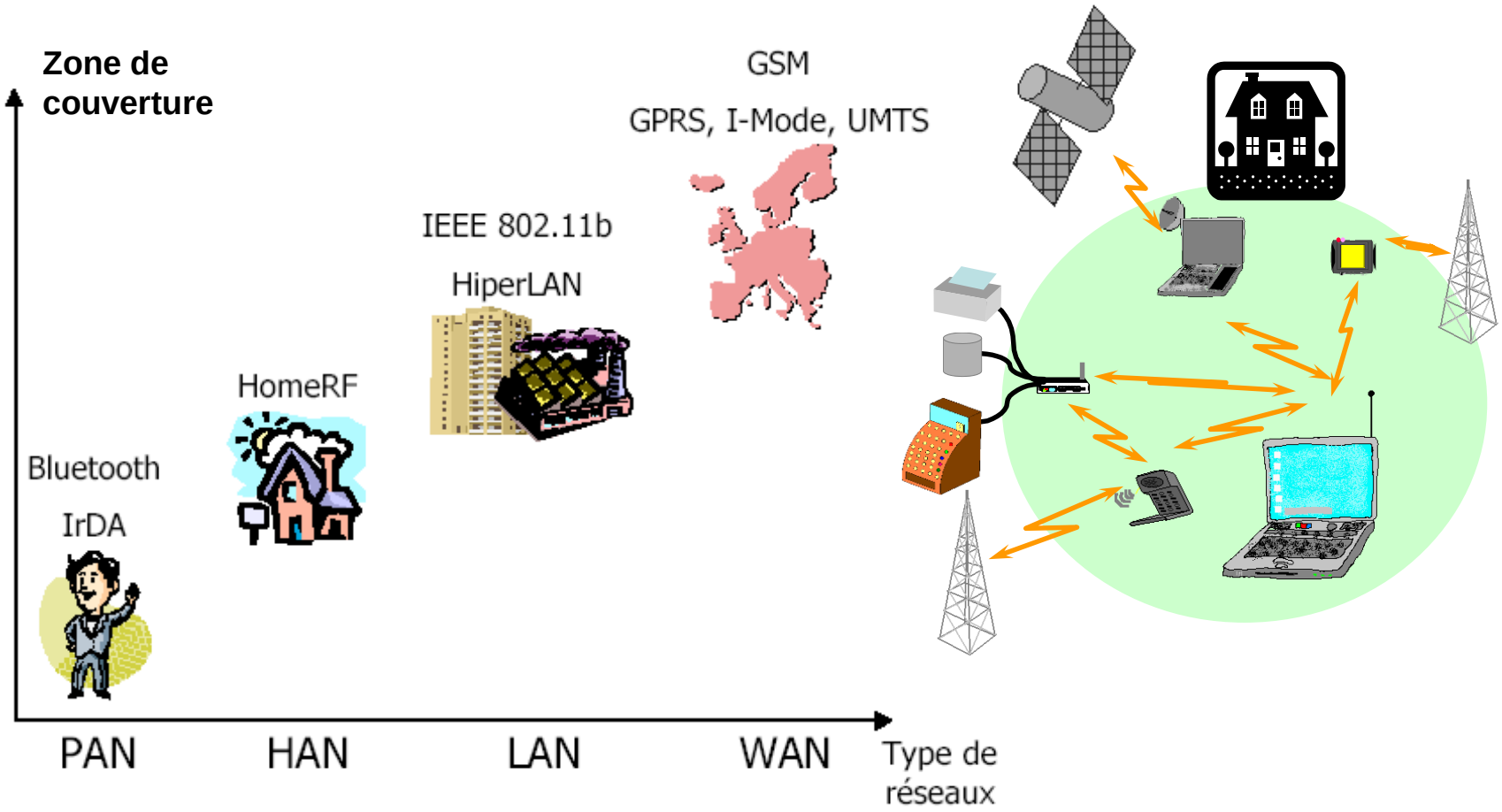
ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
August 2011

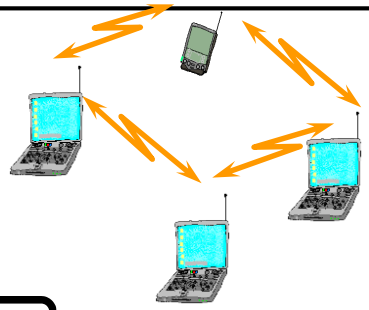
Types de réseaux sans fil

Couverture des réseaux sans fil



Couverture des réseaux sans fil

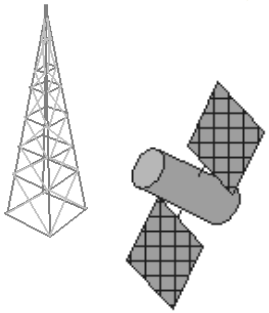
- **PAN** : Personal Area Network
  - ~ quelques mètres autour de l'usager
  - Ex : Bluetooth, IrDA



- **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

Bases de la transmission

Quelques rappels…

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

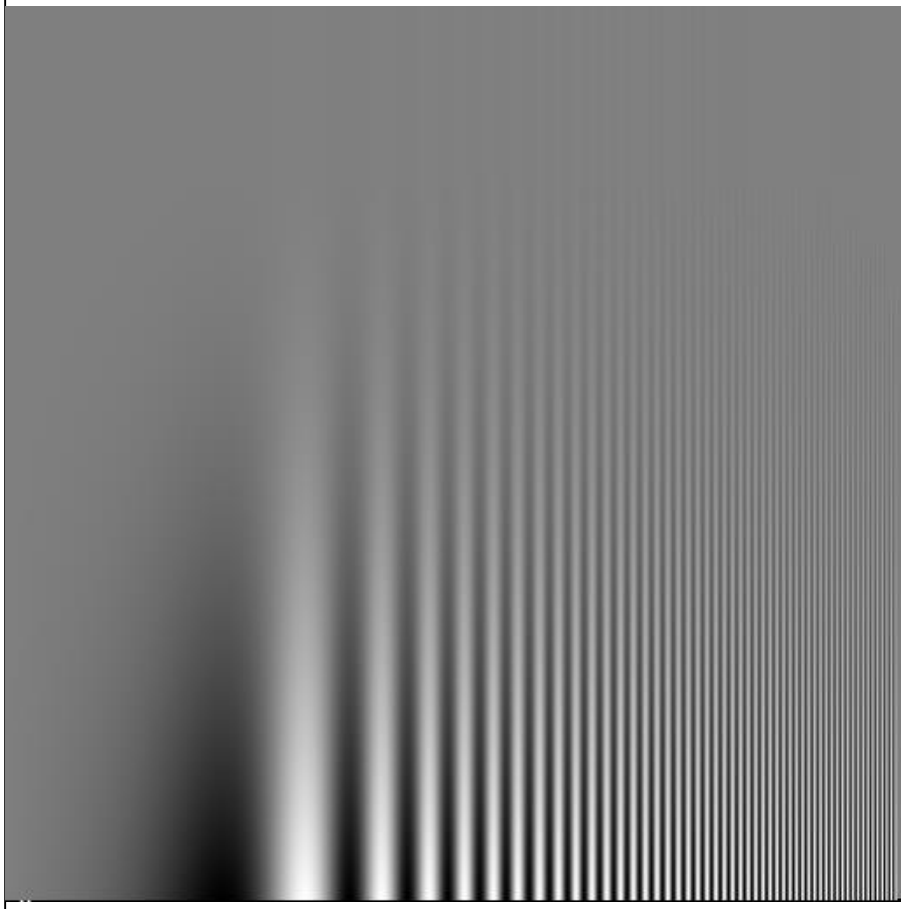
- **Transformée de Fourier**

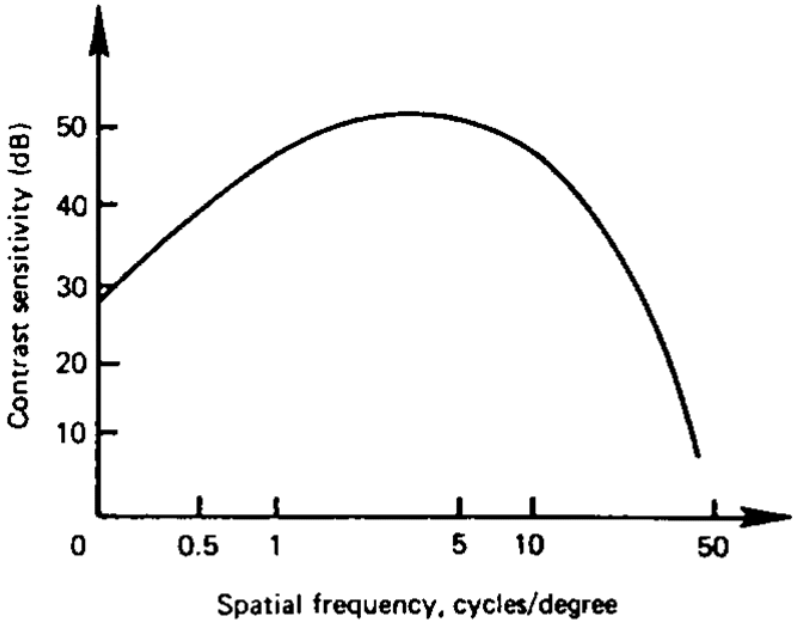
  → Représentation d'un signal sur une base de fonctions exponentielles complexes

  – Cas mono-dimensionnel

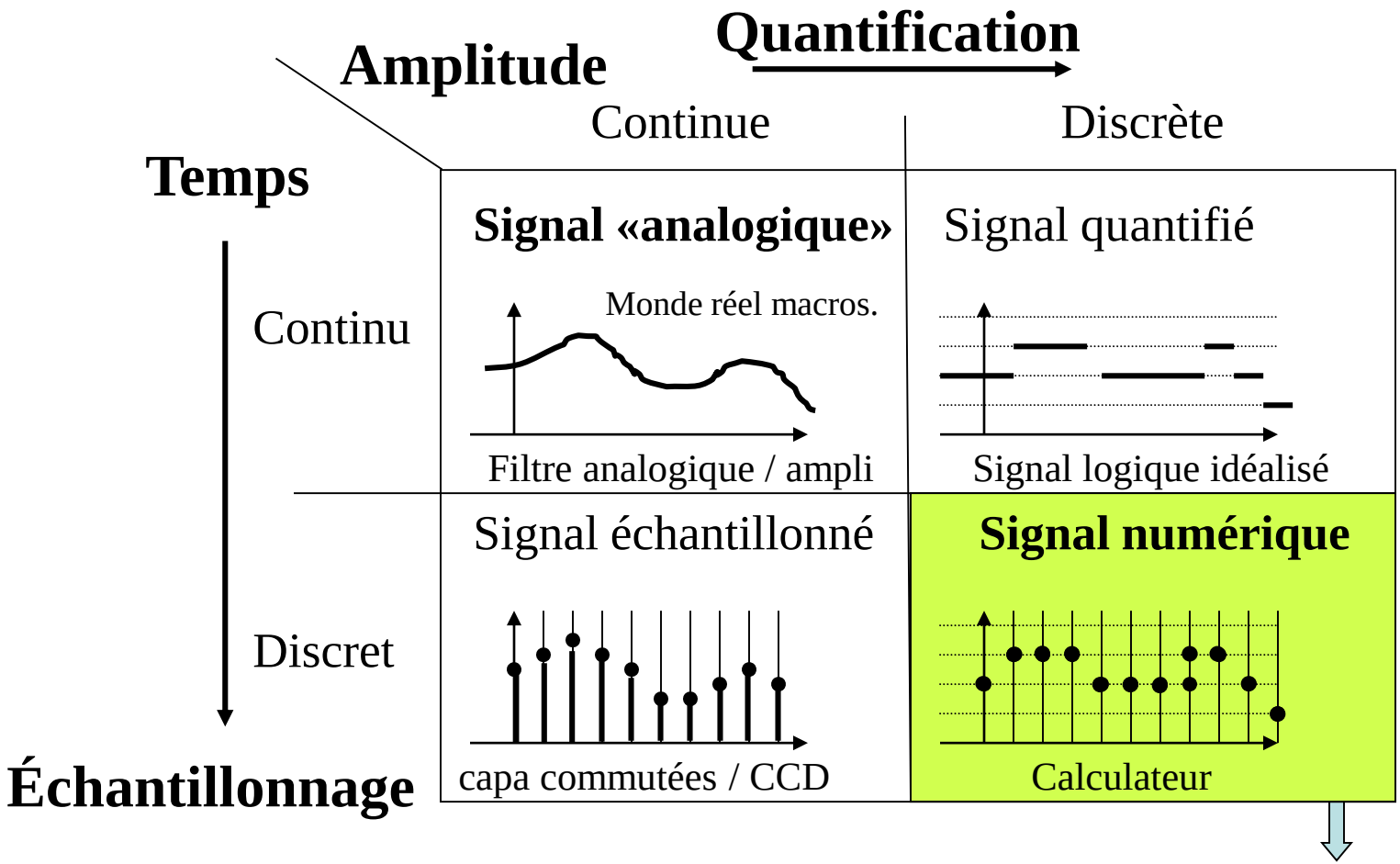
$$f(x) = \int_{-\infty}^{+\infty} F(u).e^{2\pi jux} du \qquad \xrightarrow{F} \qquad \xleftarrow{F^{-1}} \qquad F(u) = \int_{-\infty}^{+\infty} f(x).e^{-2\pi jux} dx$$

Exemple : réponse en fréquence de l'oeil





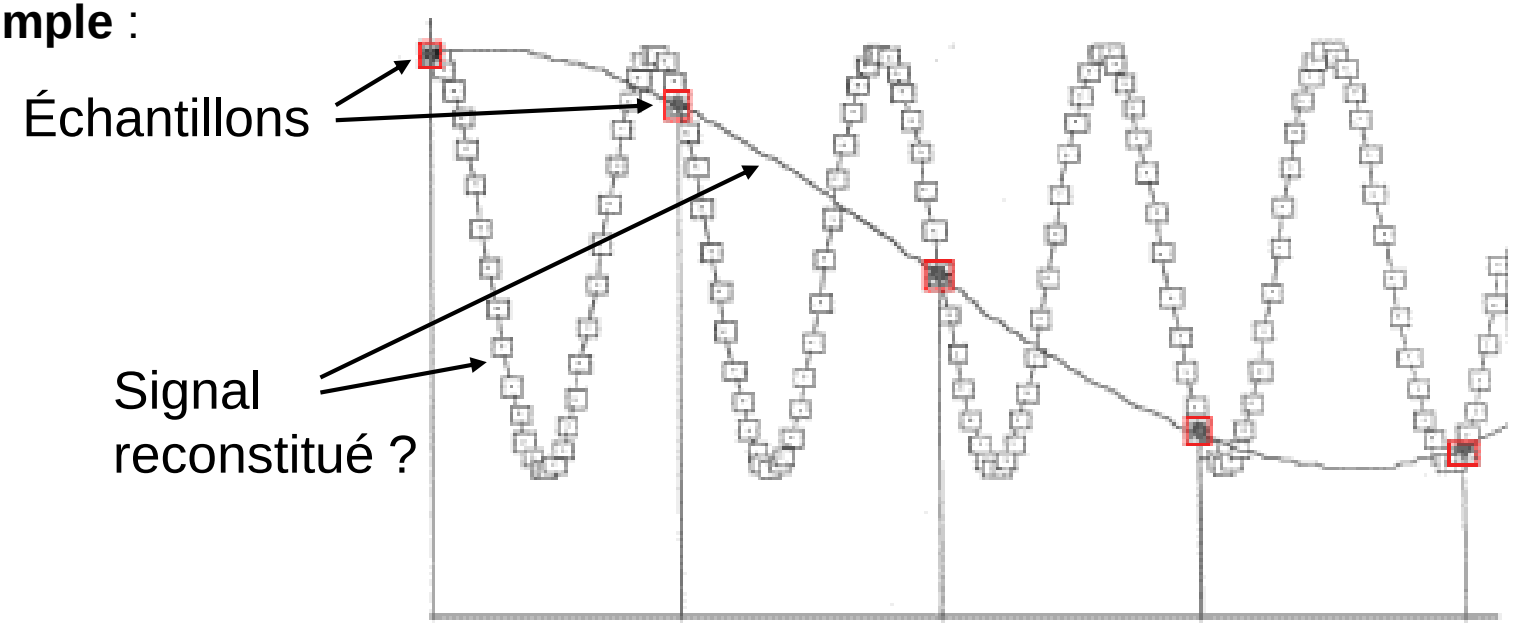
Numérisation / discrétisation



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

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

Exemple :



Un signal incorrectement échantillonné ne pourra pas être reconstitué

Bande passante

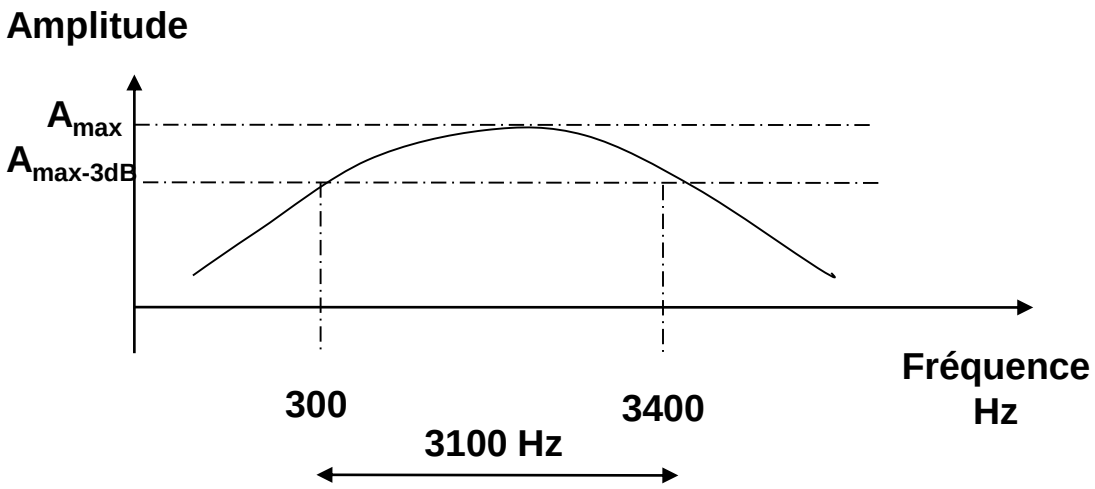
La **bande passante** caractérise tout support de transmission, c'est la bande de fréquences dans laquelle les signaux sont correctement reçus :

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)

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

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 $\Rightarrow$ 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 :

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

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

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

- **<u>Exemple</u>**: 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 $\Rightarrow$ 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**

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

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

- Affaiblissements différents suivant les harmoniques $\Rightarrow$ **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 $\Rightarrow$ 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 :

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

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

Modulation / Démodulation

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

$\Rightarrow$ 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.

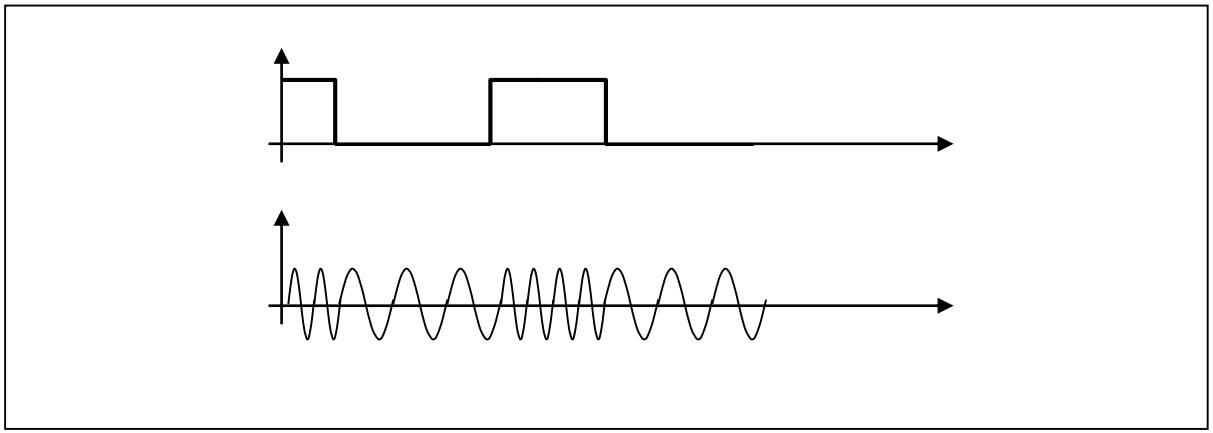
Modulation

- ***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)

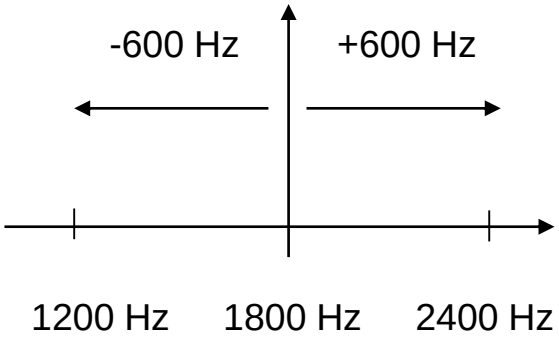
- une valeur de fréquence $\leftrightarrow$ une valeur du signal



Modulation de fréquence

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

$\Rightarrow$ une fréquence est associée à chaque niveau logique.



Modulation de fréquence

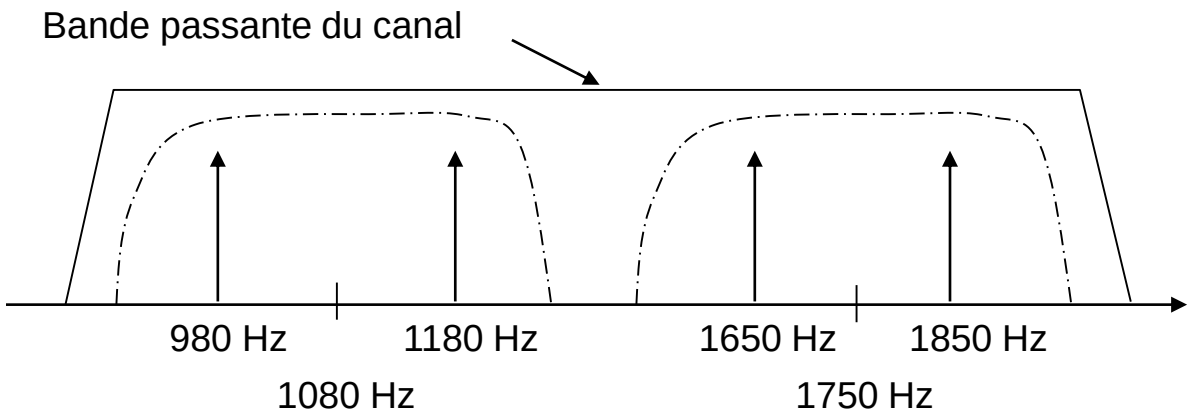
- Liaison "full-duplex":

  Émission / Réception simultanée

⇒ on partage la bande passante du canal

une voie à l'émission F_1 +/- f_1

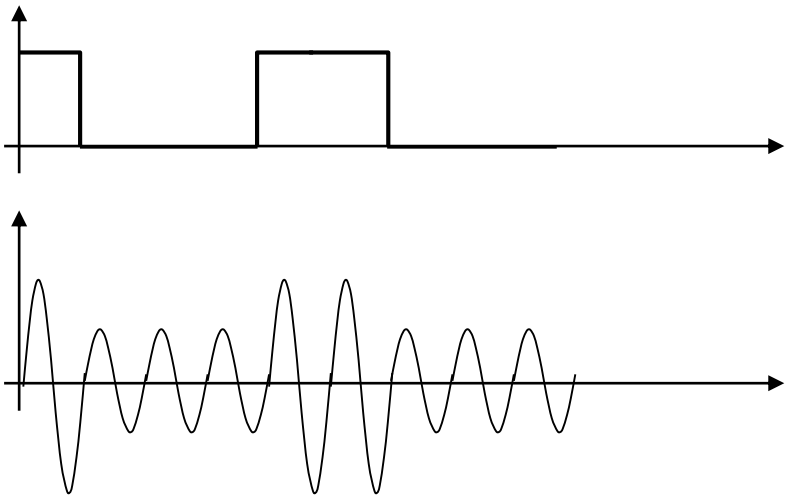
+ une voie à la réception F_2 +/- f_2



Modulation d'amplitude

(ASK: Amplitude Shift Keying)

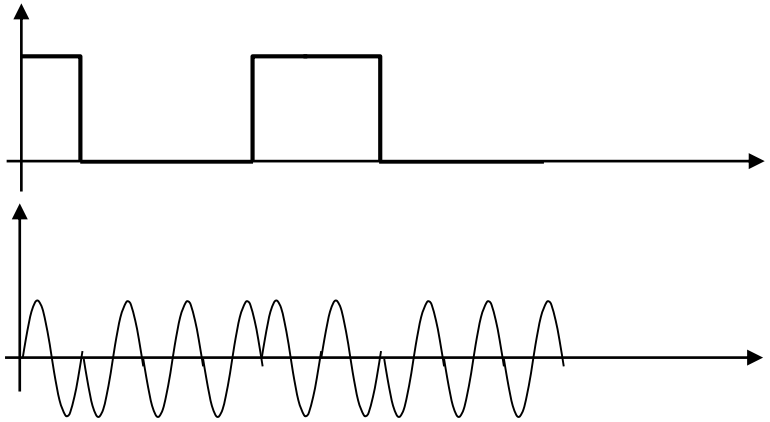
- une valeur d'amplitude ↔ une valeur du signal



Modulation de phase

(PSK: Phase Shift Keying)

- un déphasage ↔ une valeur du signal

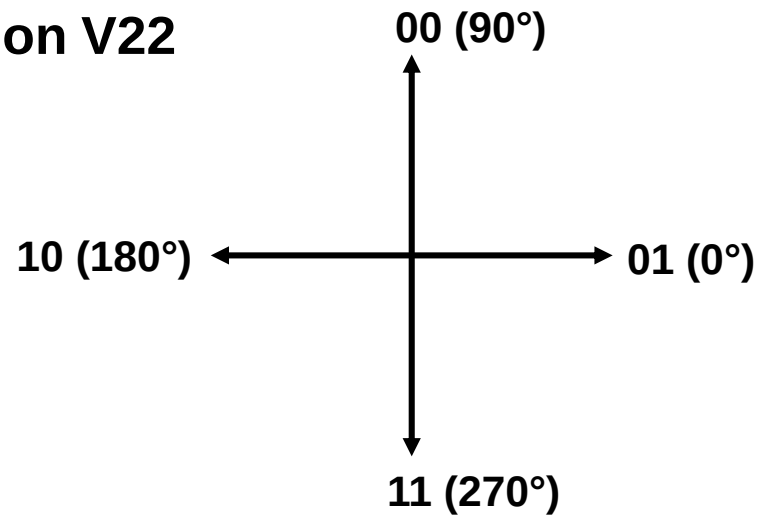


- Avec des codes à plusieurs bits, on peut augmenter le débit sans changer la fréquence de modulation.
- Les vitesses de transmission sont plus élevées qu'en modulation FSK pour la même bande passante

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

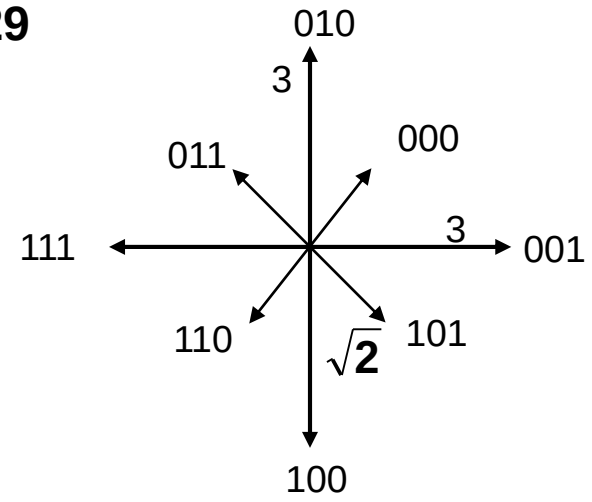
- Combiner plusieurs types de modulation parmi les trois types de modulation décrits auparavant.

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

Exemple : Modulation V29 à 7200 bits/s

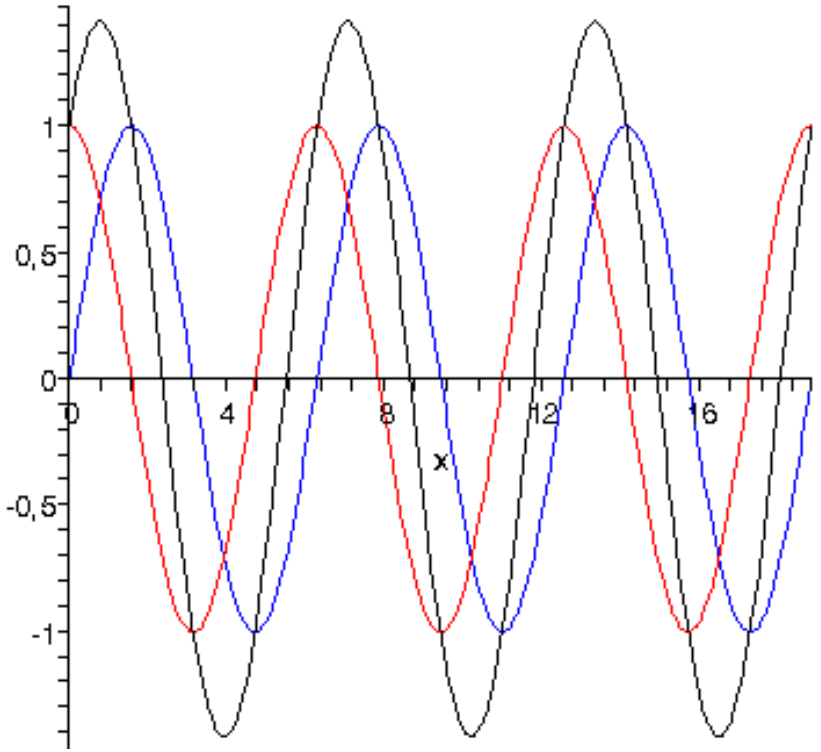
- 8 états de phase et 2 valeurs d'amplitude

Constellation V29



Modulation combinée en quadrature

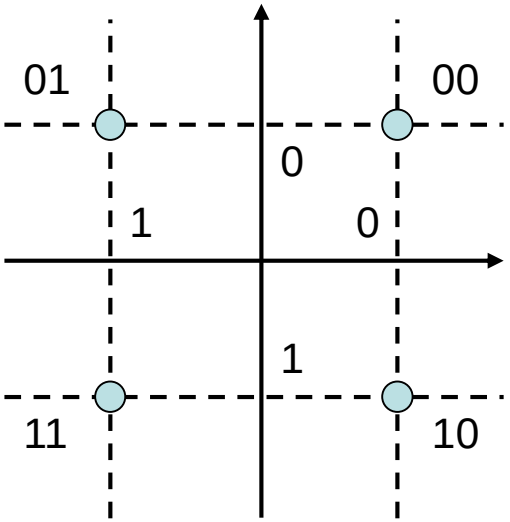
- Porteuses en quadrature : addition de deux porteuses de fréquence f_0 en quadrature, on obtient une seule porteuse, toujours de fréquence f_0



Modulation combinée en quadrature

Modulation de phase

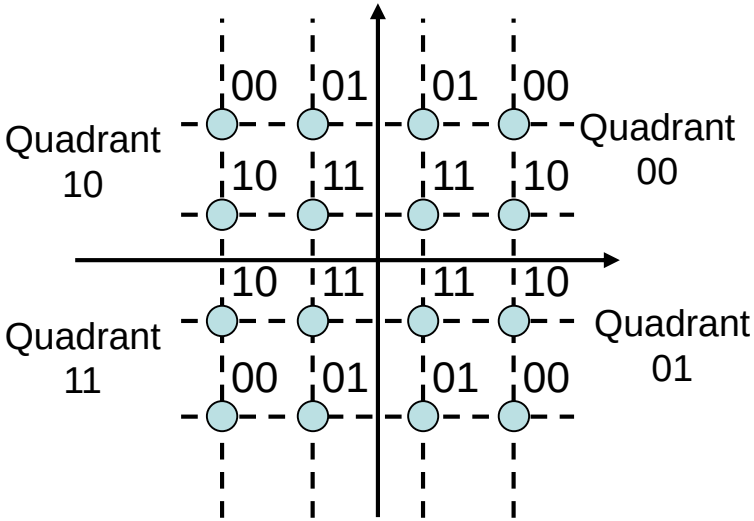
4 états (2 bits)



Quadrature Amplitude Modulation

QAM 16

16 états (4 bits)



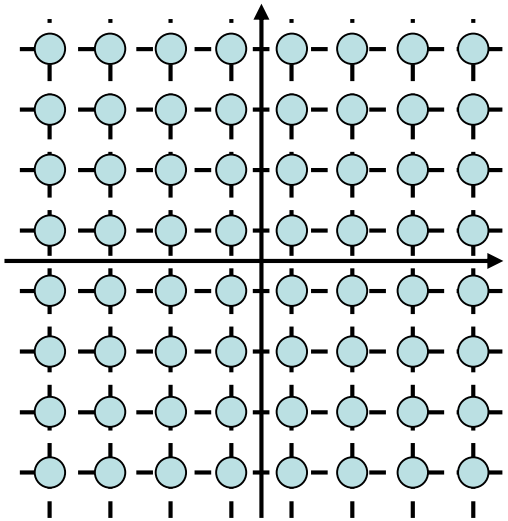
Modulation des 2 porteuses

Modulation combinée en quadrature

Quadrature Amplitude Modulation

QAM 64

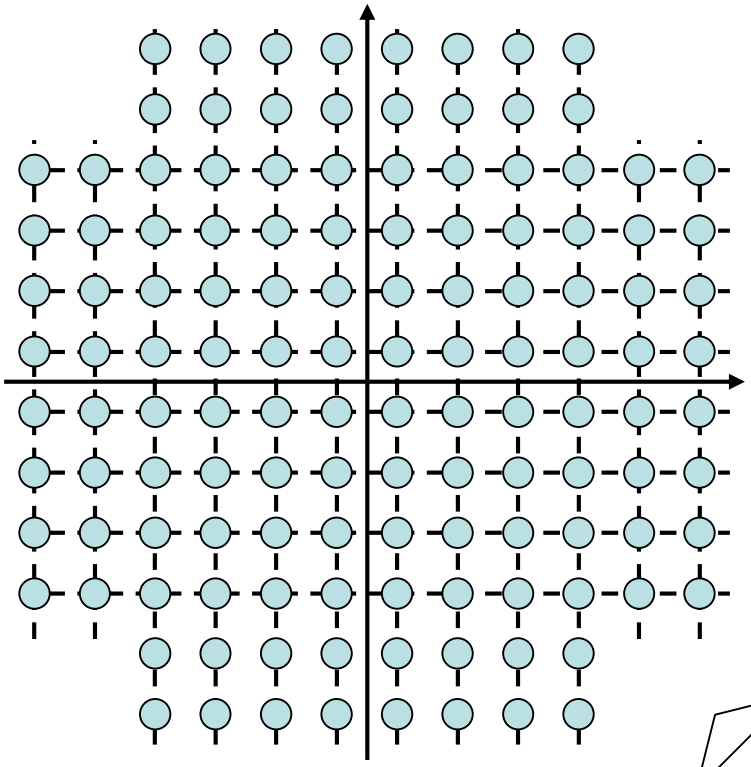
64 états (6 bits)



Quadrature Amplitude Modulation

QAM 128

128 états (7 bits)



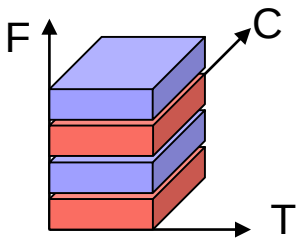
Multiplexage

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)

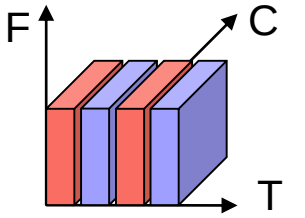
    FDM (Frequency Division Multiplexing)



  - **multiplexage temporel** :

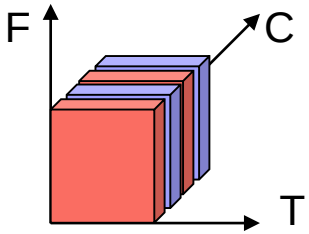
    MRT (Multiplexage à Répartition dans le Temps)

    TDM (Time Division Multiplexing)



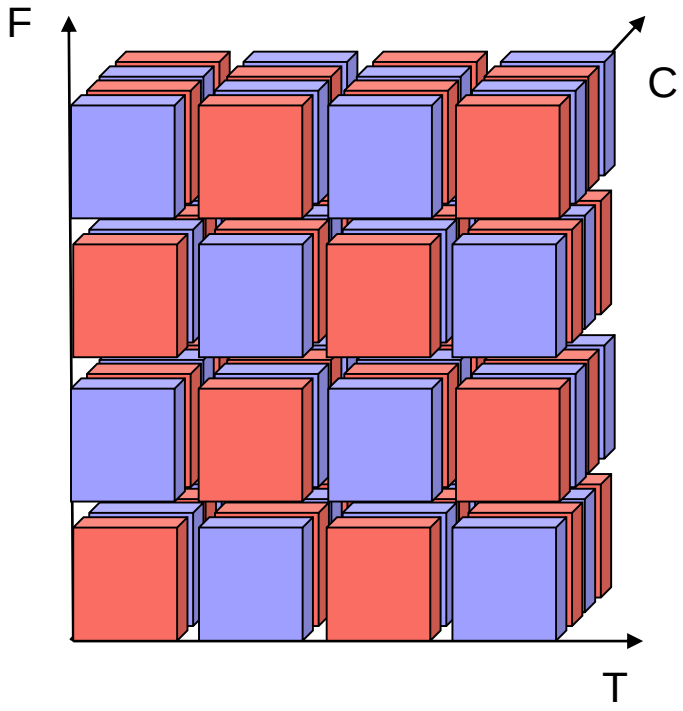
  - **multiplexage par code**

    CDM (Code Division Multiplexing)



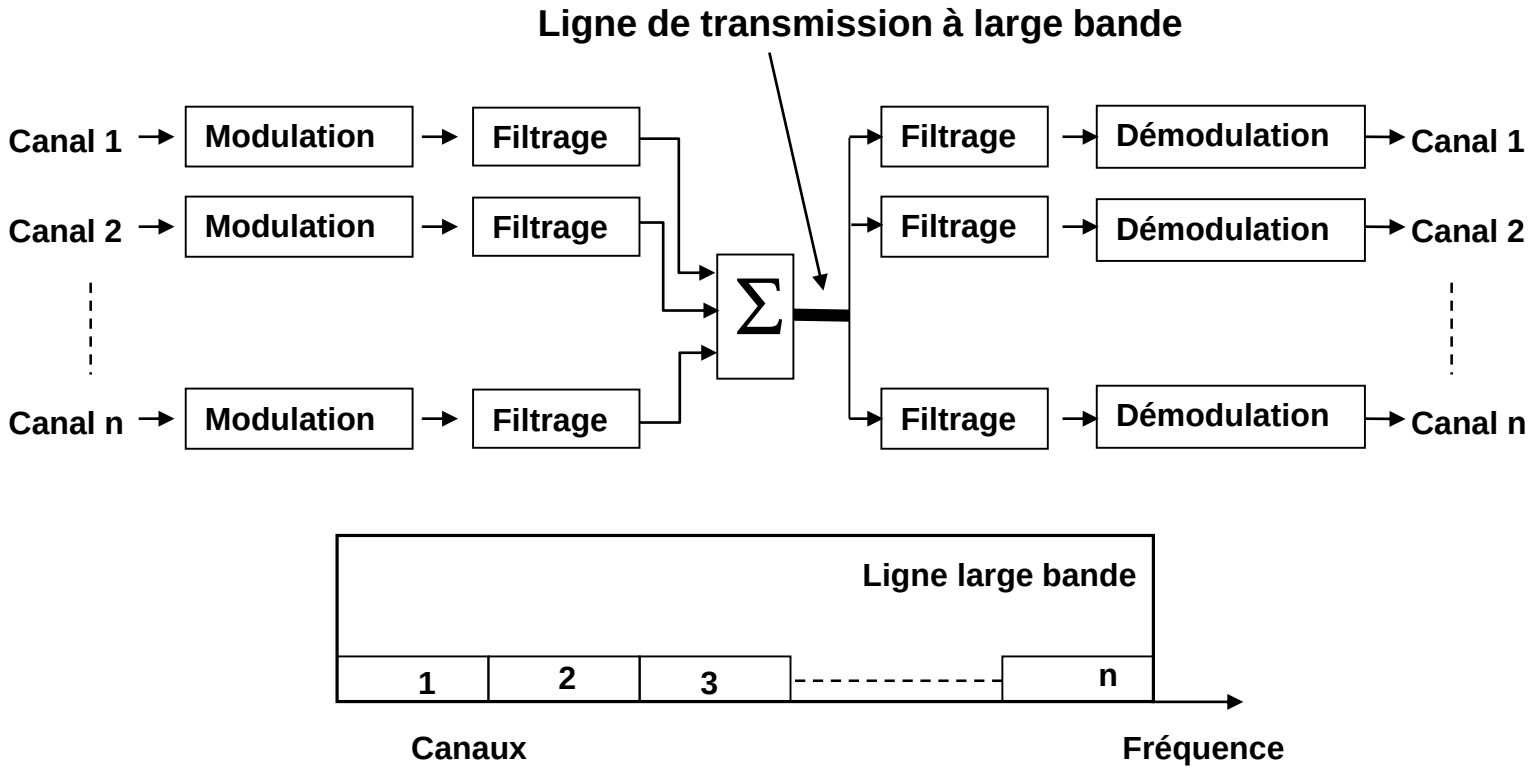
Multiplexage xDMA

- La réalité est parfois (?) plus complexe…



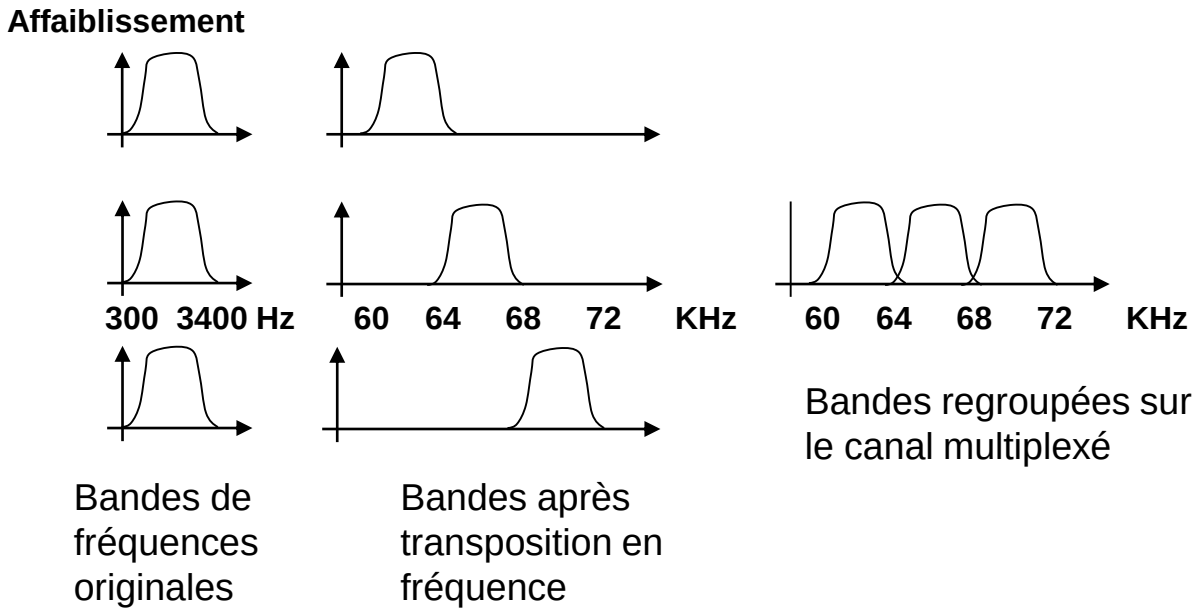
FDMA : Multiplexage en fréquences

- **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

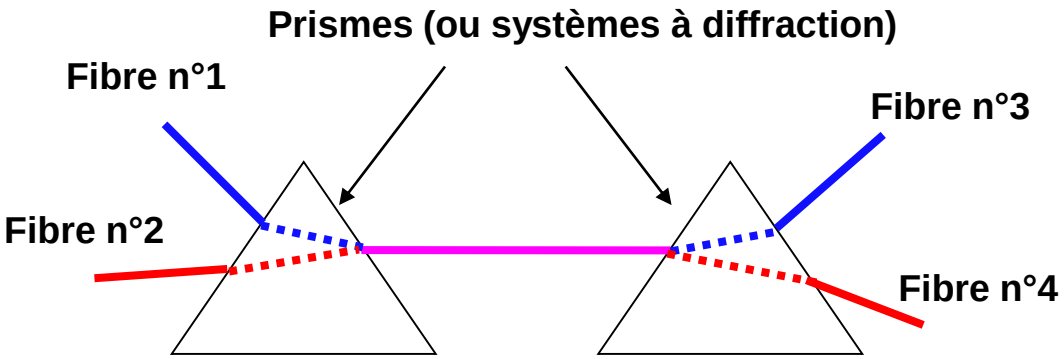
- **3 liaisons téléphoniques multiplexées avec technique FDM.**
- Des filtres appropriés limitent la bande passante à 3100 Hz par canal téléphonique.
- Pour assurer un multiplexage correct, une bande de fréquences de 4000 Hz est attribuée à chaque canal afin de bien les séparer les uns des autres.



WDMA : Multiplexage en longueur d'onde

WDM (Wavelength Division Multiplexing)

⇒ proche du multiplexage fréquentiel



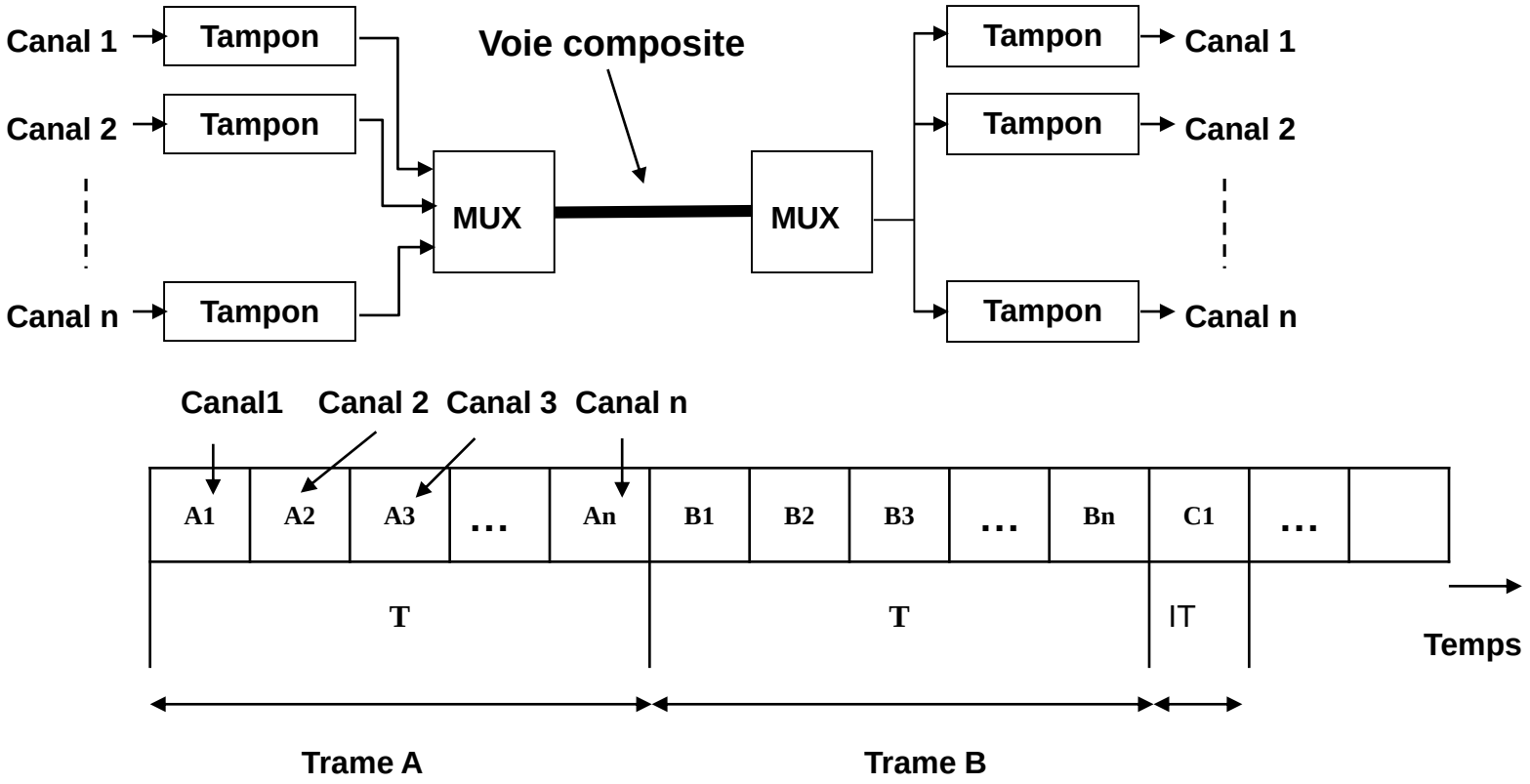
- Entrée : 2 fibres : flux lumineux d'énergie et de bande de fréquences différentes

⇒ Multiplexage WDM complètement passif ⇒ très haute fiabilité.

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

TDMA : 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

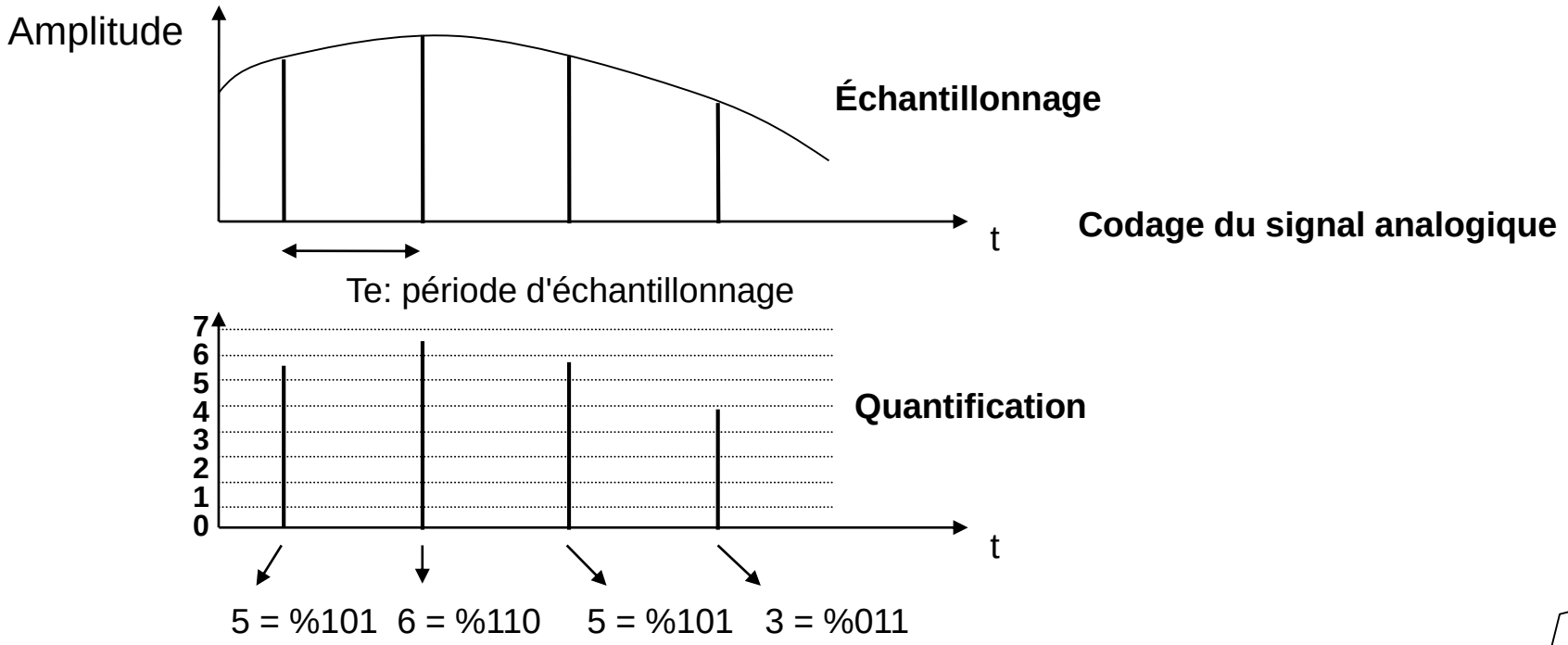
- La période *T* des trames est fonction du nombre de voies et de l'intervalle de temps élémentaire IT.

  T= n x IT

Modulation par impulsions codées (MIC)

Multiplexage temporel pour les transmissions téléphoniques.

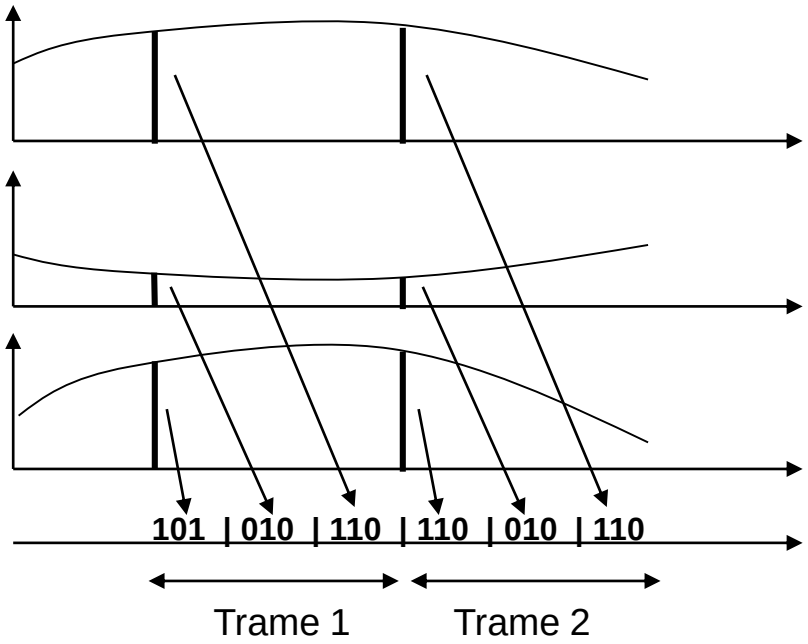
- échantillonnage des signaux analogiques de chacune des voies;
- quantification et codage des échantillons multiplexés pour obtenir un signal numérique.
- multiplexage temporel des échantillons des différentes voies;



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.**

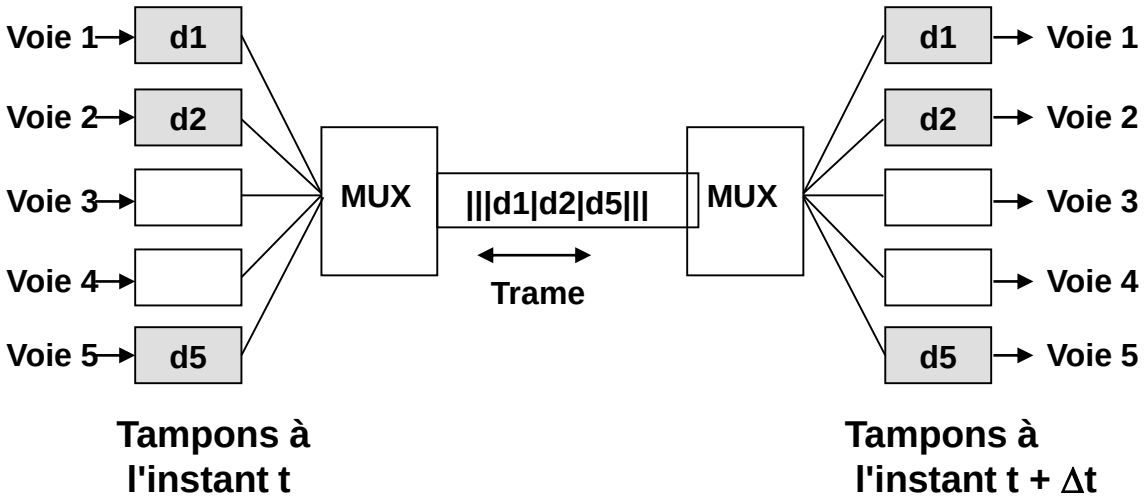
⇒ permet de raccorder plusieurs équipements sur une seule ligne, même si le débit cumulé de chaque voie est supérieur au débit maximum de la ligne.

⇒ Le multiplexeur intègre un microprocesseur et des mémoires tampon:

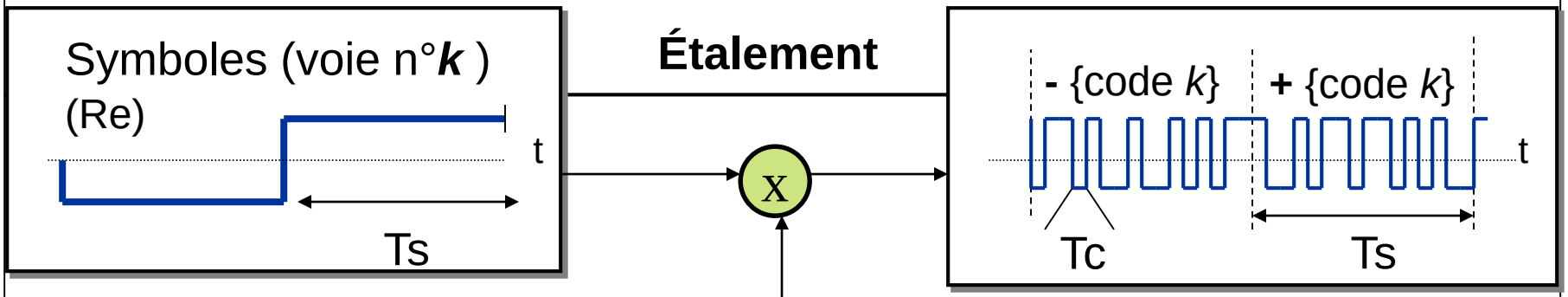
il permet **des débits et des paramètres de transmission différents sur chaque voie** ou sous-canal et à chaque extrémité.

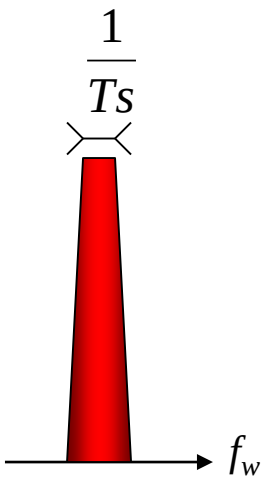
Multiplexage temporel statistique

- 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.

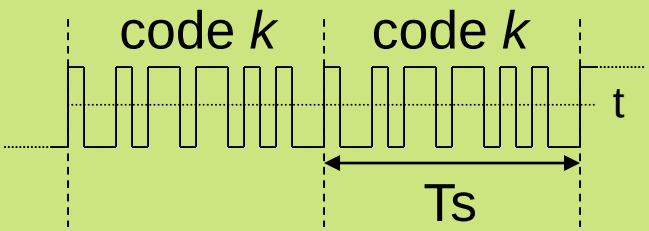


CDMA: étalement de spectre par code





Spectre original



Séquence d'étalement:
code **k** périodisé au temps Ts

1 symbole ➔ Q chips
Q: facteur d'étalement

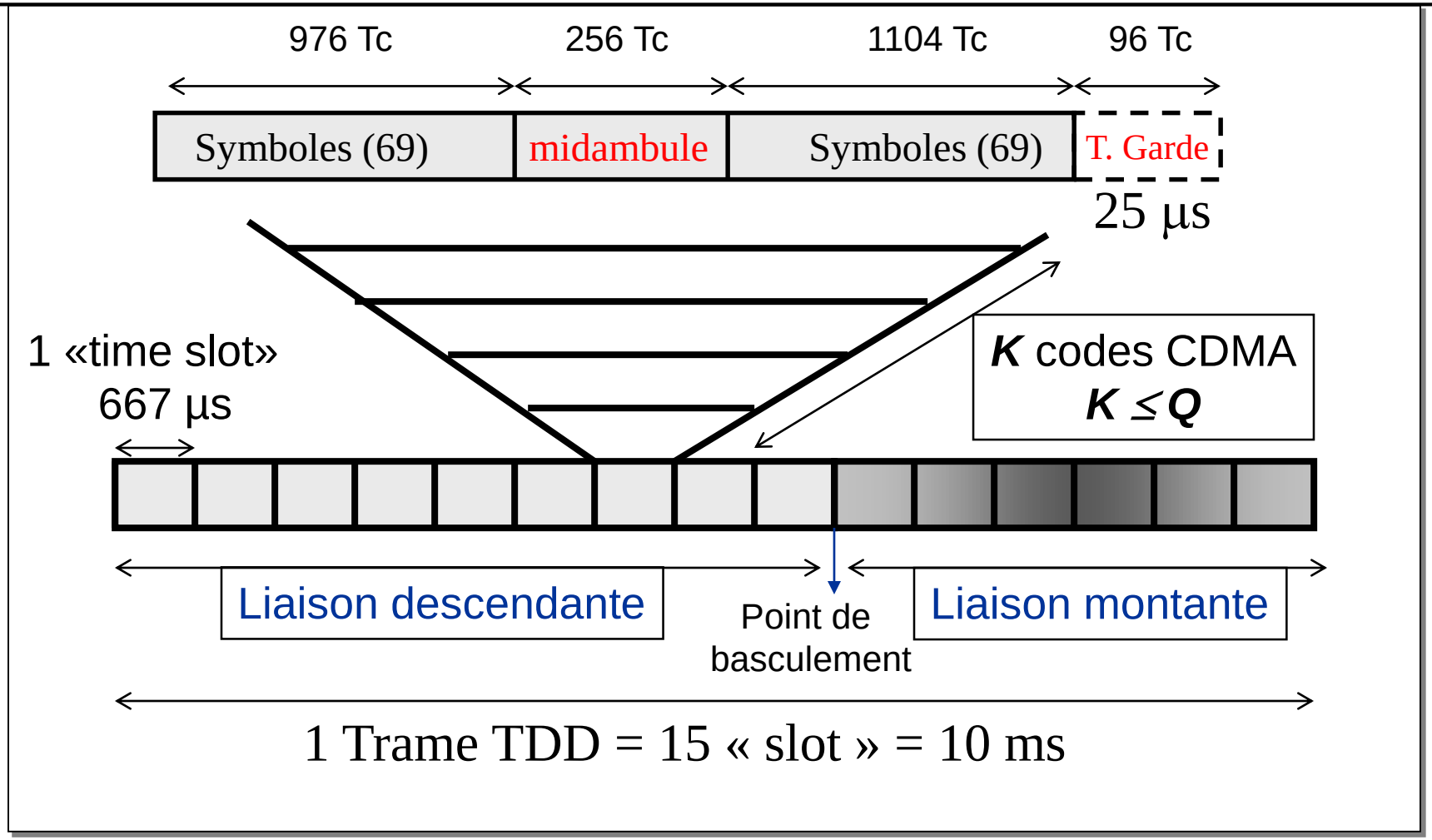
$$\frac{1}{Tc} = Q.\frac{1}{Ts}$$

Spectre après étalement

mode TDD de l'UMTS (2)

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

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



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

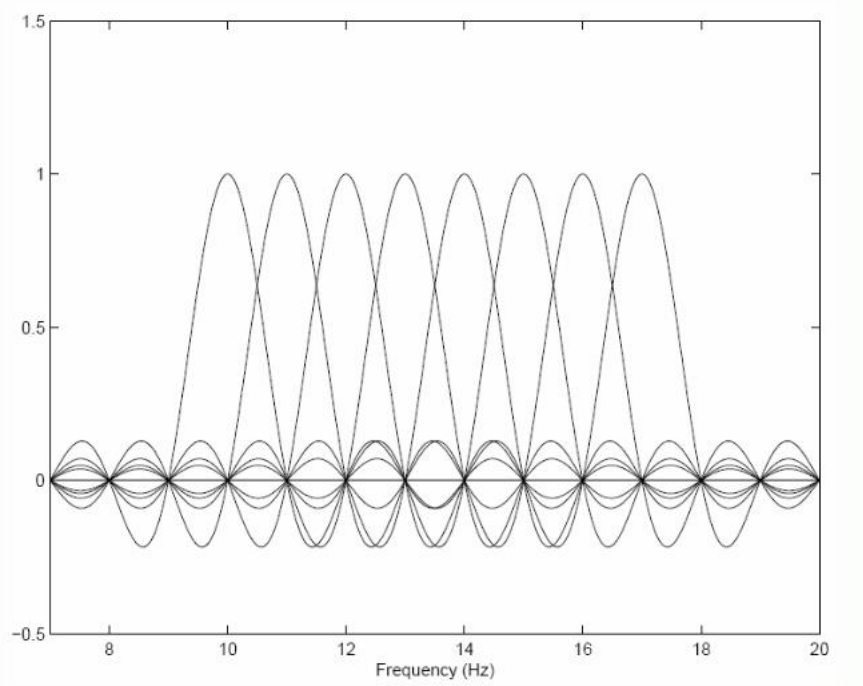
OFDM : Modulation multi-porteuses

$$\mathrm{DFT}\{x[n]\} = X[i] \triangleq \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} x[n] e^{-j\frac{2\pi ni}{N}}, \quad 0 \leq i \leq N-1.$$

$$\mathrm{IDFT}\{X[i]\} = x[n] \triangleq \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} X[i] e^{j\frac{2\pi ni}{N}}, 0 \leq n \leq N-1.$$

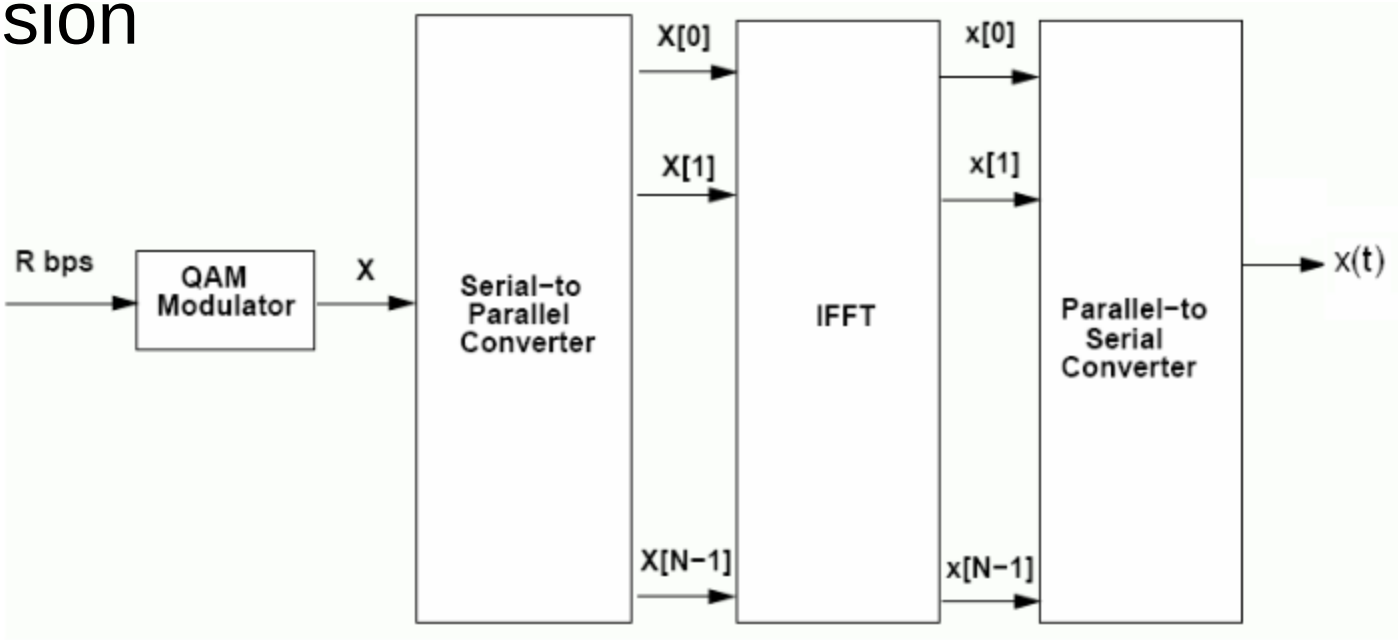
OFDM : Modulation multi-porteuses

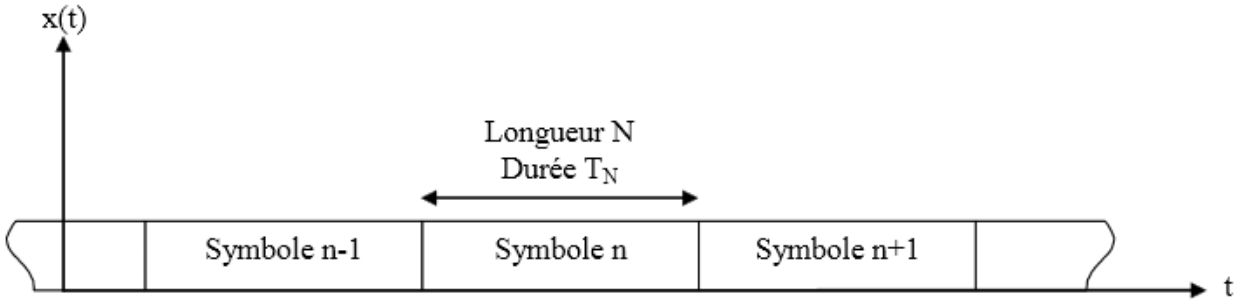
- Multi-porteuses avec recouvrement



OFDM : Modulation multi-porteuses

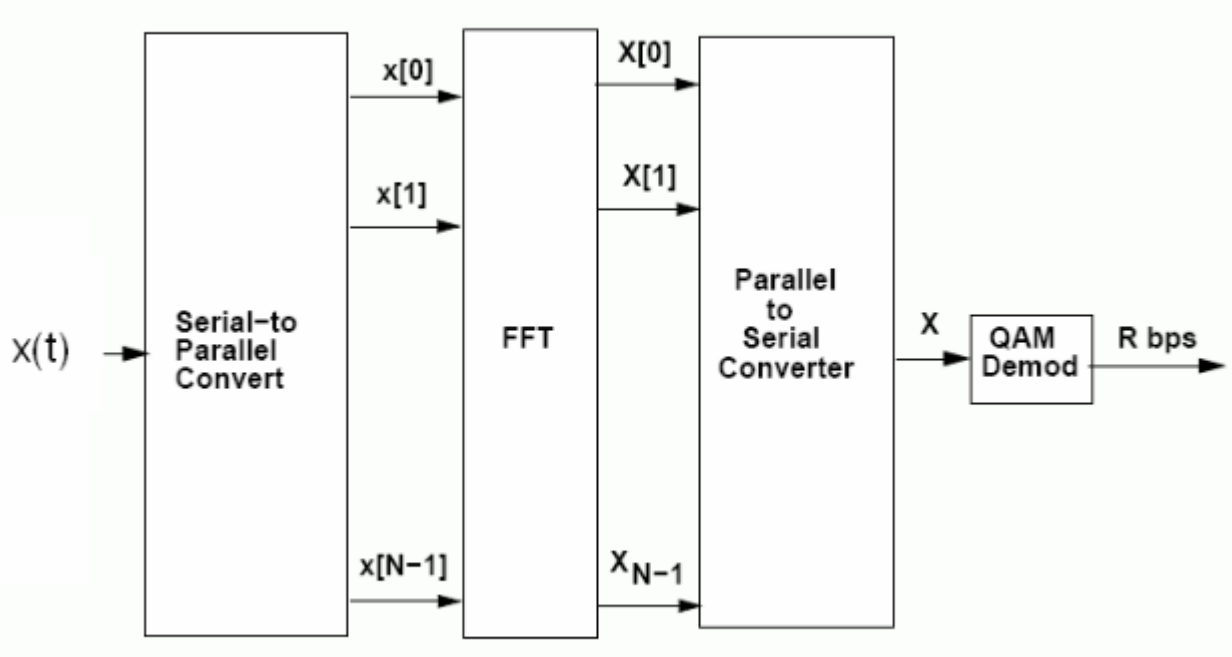
- Emission



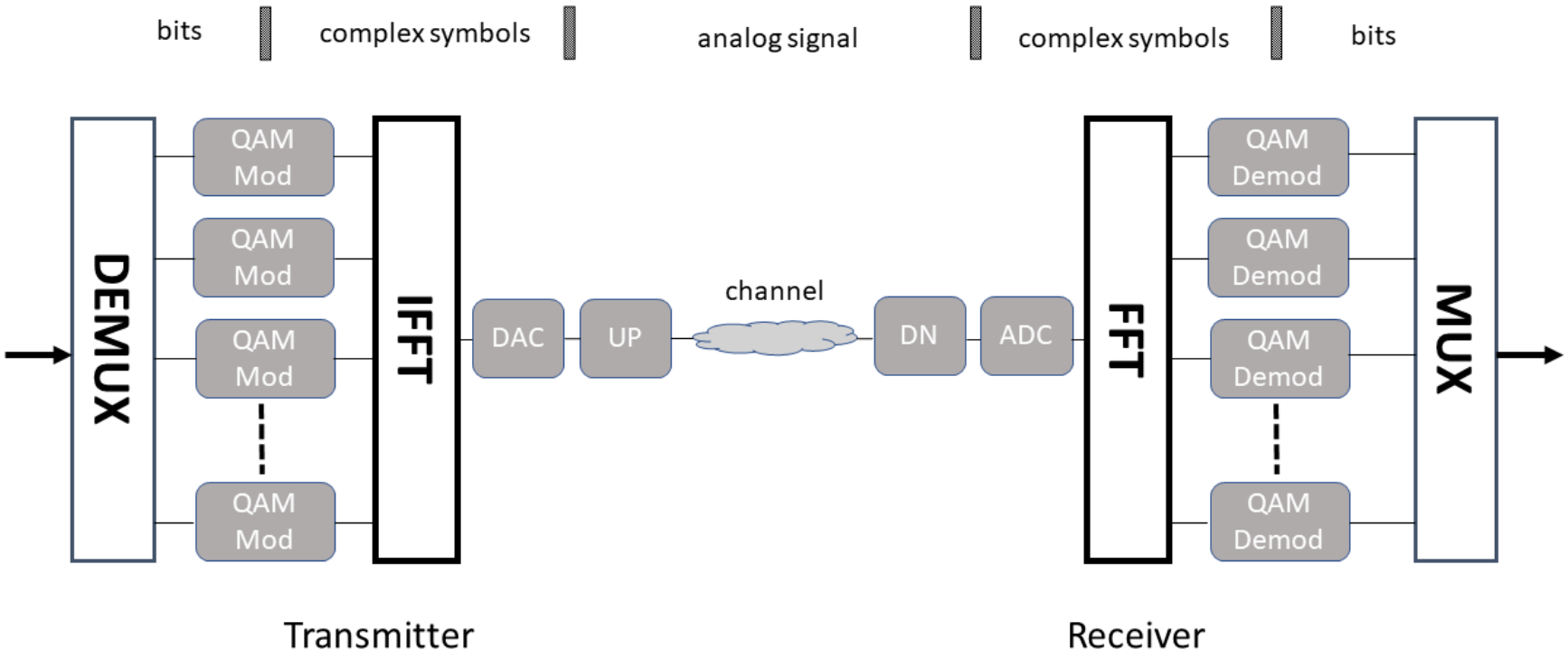


OFDM : Modulation multi-porteuses

- Réception



OFDM


bits
complex symbols
analog signal
complex symbols
bits
DEMUX
QAM Mod
QAM Mod
QAM Mod
QAM Mod
IFFT
DAC
UP
channel
DN
ADC
FFT
QAM Demod
QAM Demod
QAM Demod
QAM Demod
MUX
Transmitter
Receiver

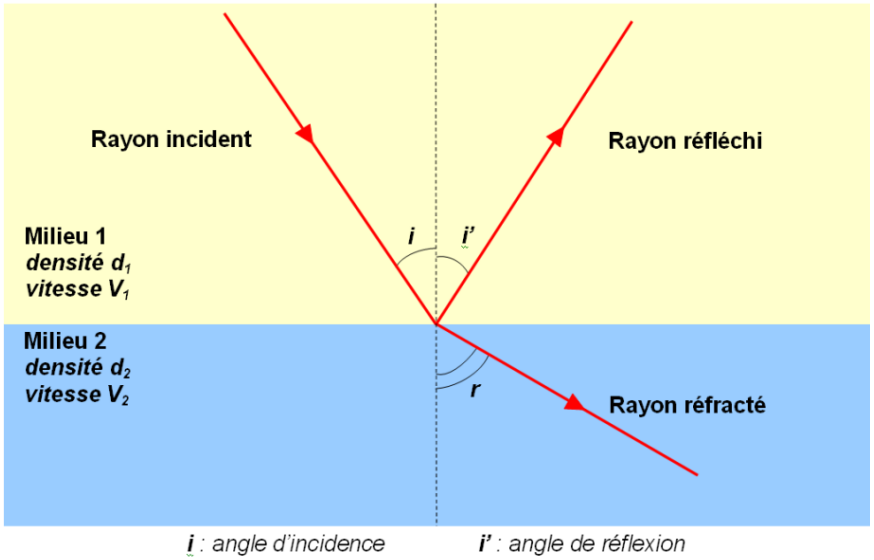
Cartes

- Carte des émetteurs / mesures
  - https://www.cartoradio.fr
- Carte des Faisceaux Hertziens
  - https://carte-fh.lafibre.info/

Propagation

Onde radio

- Propagation en ligne droite depuis la source d'émission, dans une ou plusieurs directions
- Vitesse dans le vide ~3.10^8 m/s
- Si l'onde rencontre un obstacle, son énergie se partage entre l'onde réfléchie, réfractée et absorbée :



Gain et atténuation

- Le gain ou l'atténuation est égal au rapport entre la puissance du signal avant et après modification (obstacle, antenne, propagation, etc.)

- Atténuation ou gain = $10 * \log (S_2/S_1)$

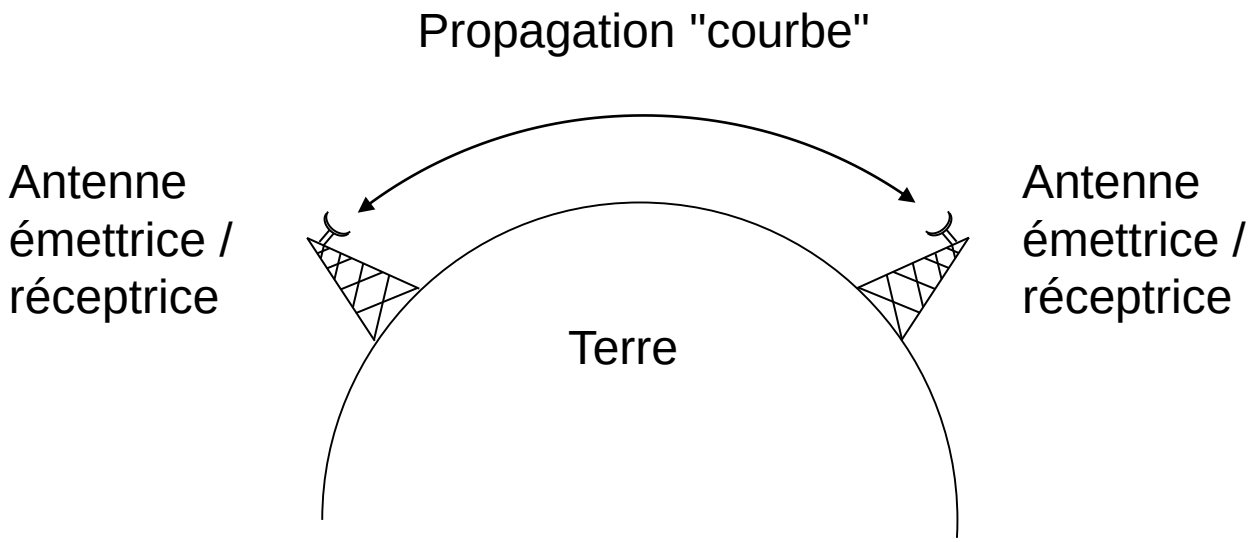
Gain d'antenne

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

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

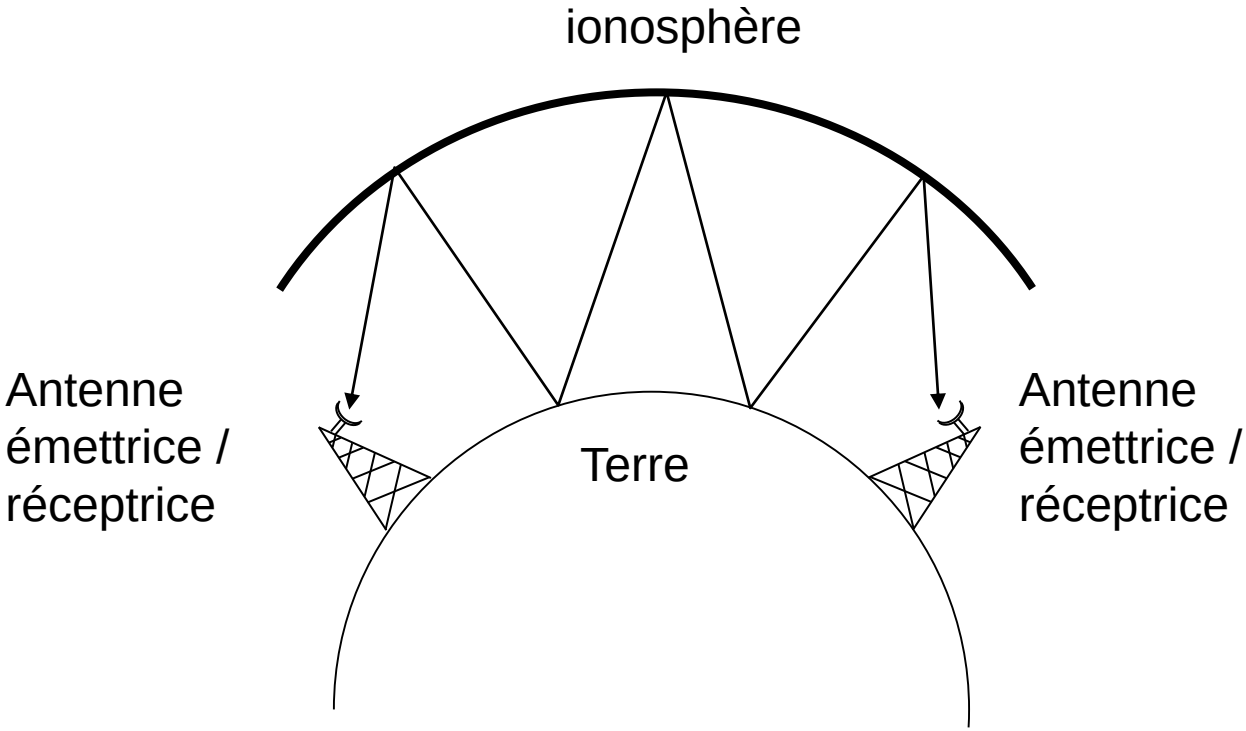
  - G = gain
  - A_e=surface effective
  - f = fréquence de la porteuse
  - c = vitesse de la lumière 3.10^8 m/s
  - λ= longueur d'onde de la porteuse

Propagation par onde de sol



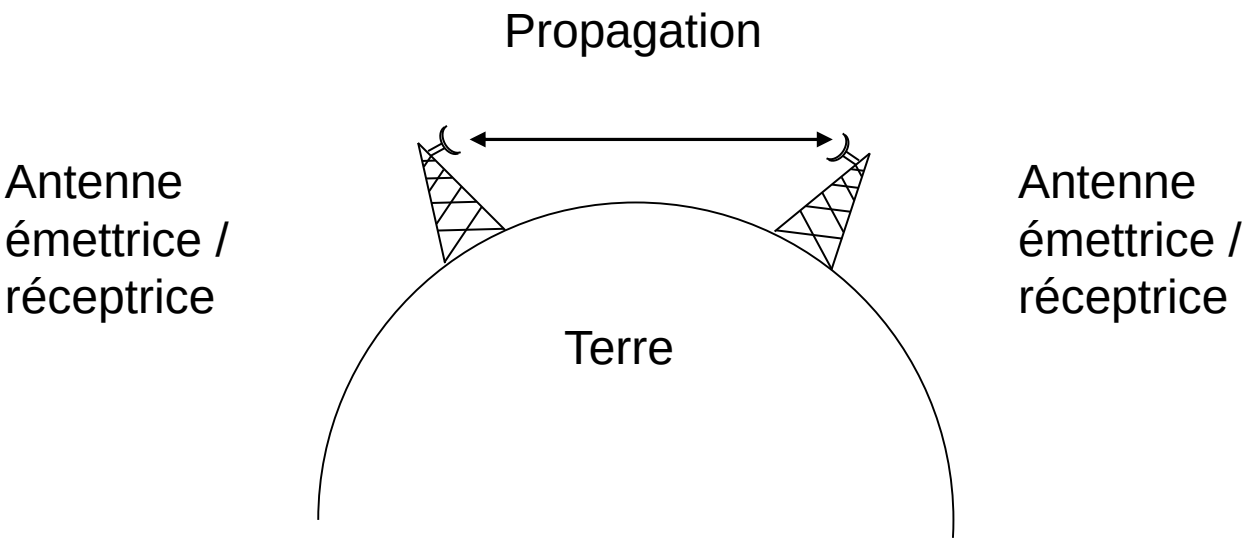
- Suit la courbure de la terre
- Grandes distances
- Fréquence -> 2 MHz
- Exemple Radio AM

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 :

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

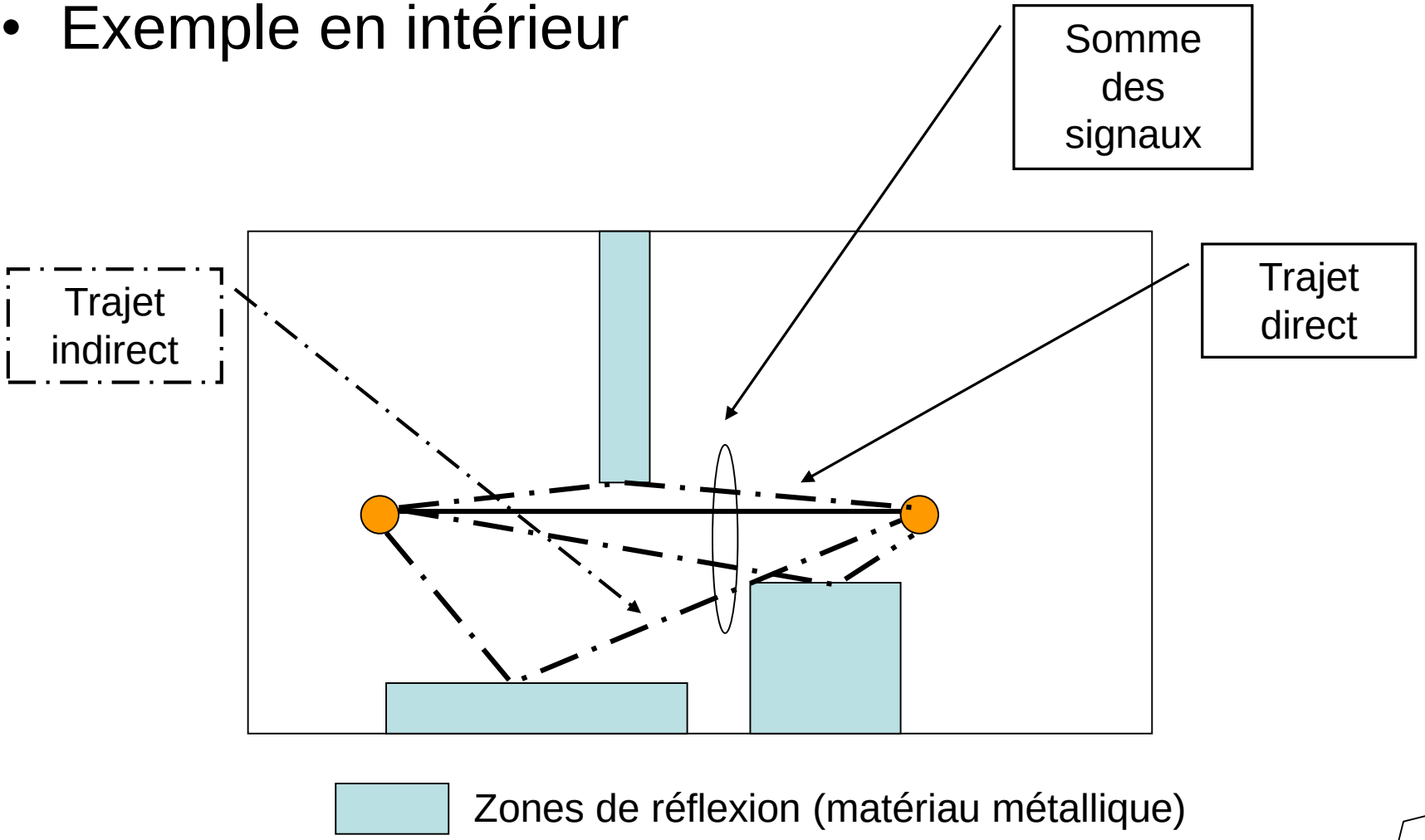
$$L_{(dB)} = 20\,log(\lambda) + 20\,log(d) - 10\,log(A_e A_r)$$

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

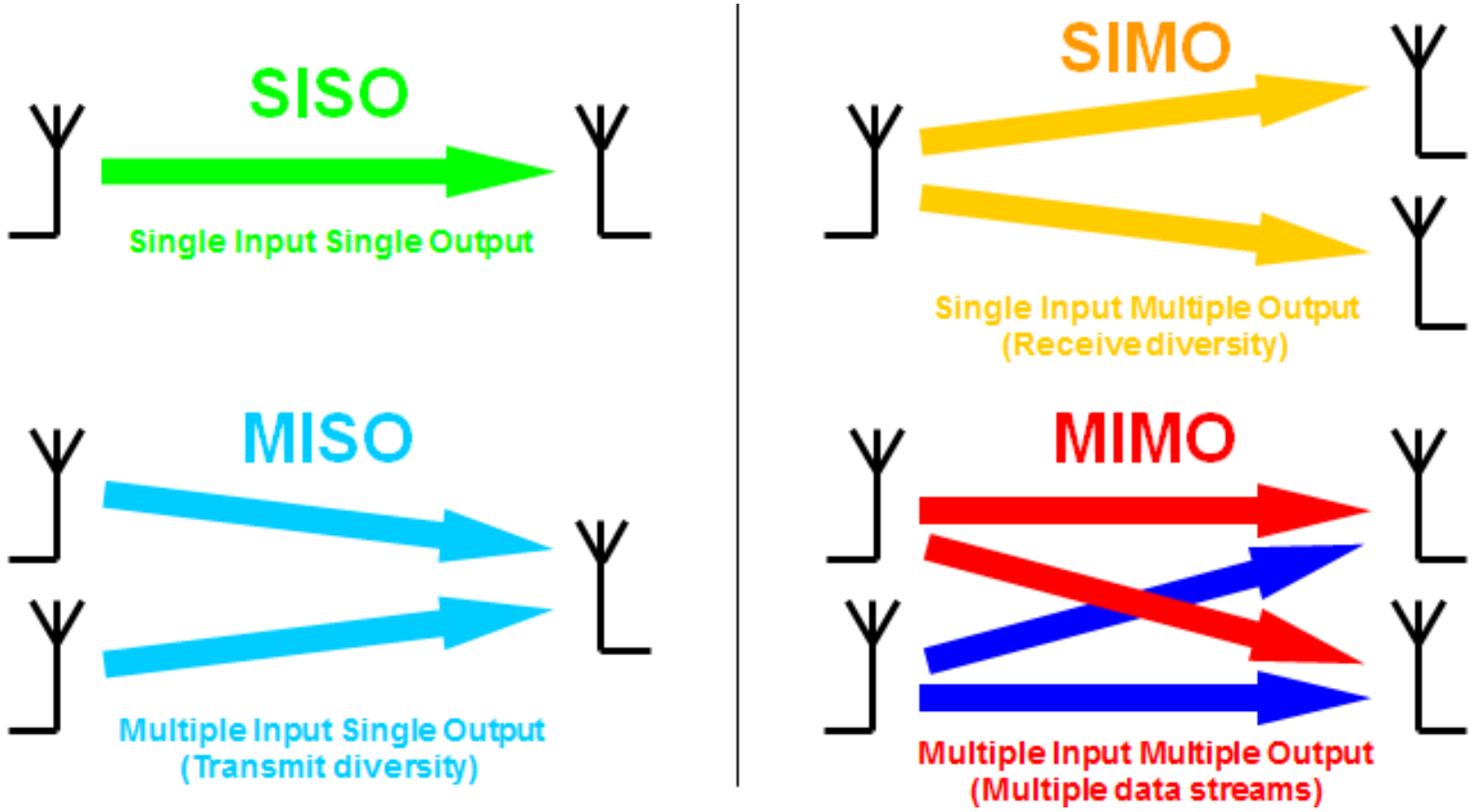
  - G_e = gain de l'antenne d'émission
  - G_r = gain de l'antenne de réception
  - A_e = surface effective de l'antenne d'émission
  - A_r = surface effective de l'antenne de réception

Notion de multi-trajets

- Exemple en intérieur

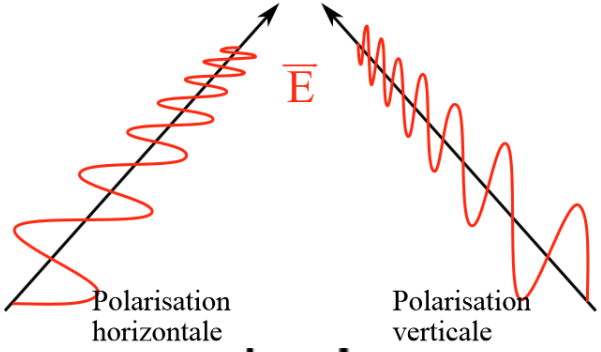


MIMO


SISO
Single Input Single Output
SIMO
Single Input Multiple Output
(Receive diversity)
MISO
Multiple Input Single Output
(Transmit diversity)
MIMO
Multiple Input Multiple Output
(Multiple data streams)

MIMO

- Polarisation des antennes
- En fonction des angles d'arrivée :
  décalage temporel
  mesure de corrélation entre antennes



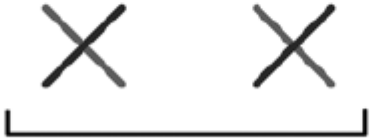
2 antennes


(1) antennes à polarisation croisée


(2) antennes copolarisées faiblement espacées

4 antennes


(3) antennes à polarisation croisée faiblement espacées

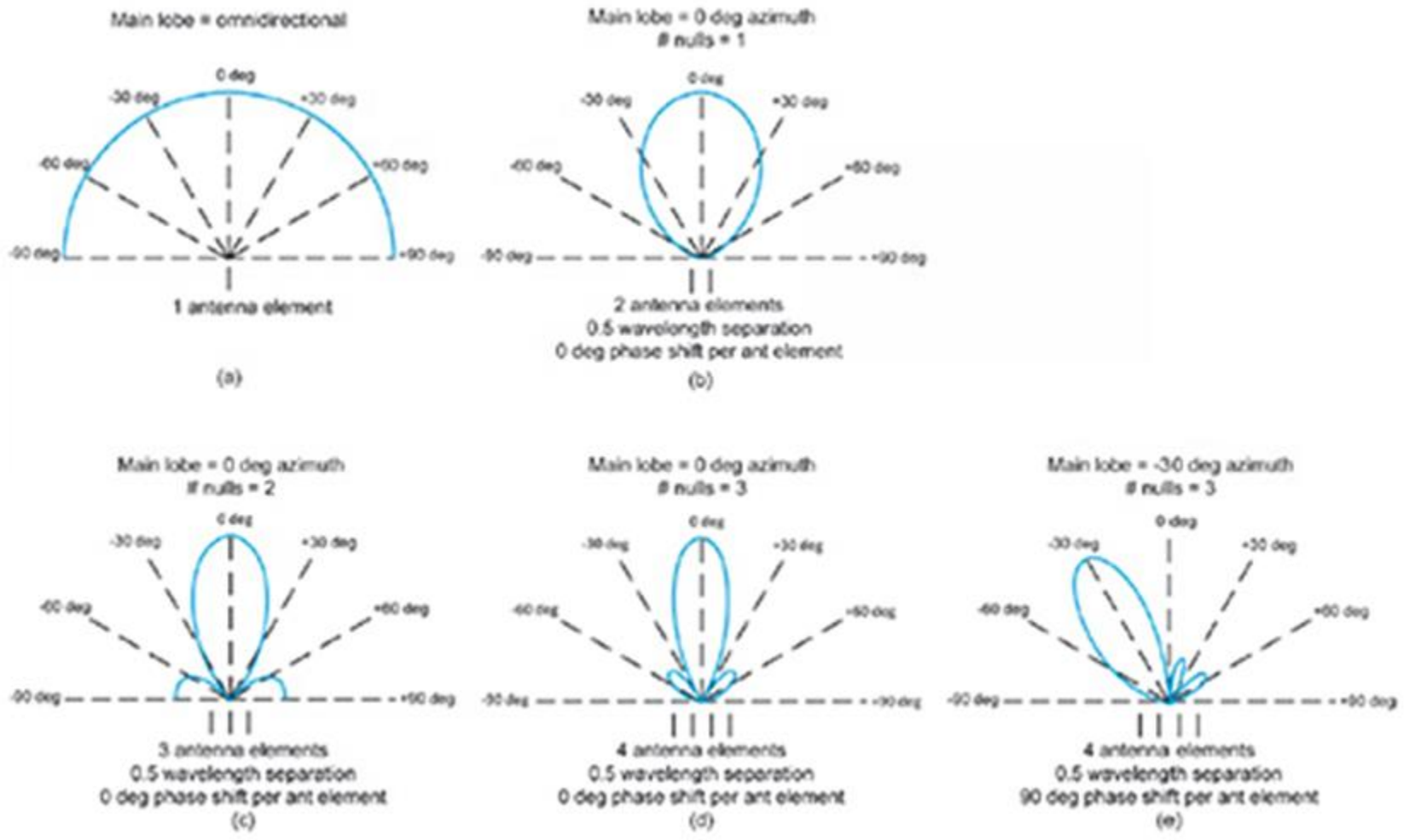

(4) antennes à polarisation croisée largement espacées


(5) antennes copolarisées faiblement espacées

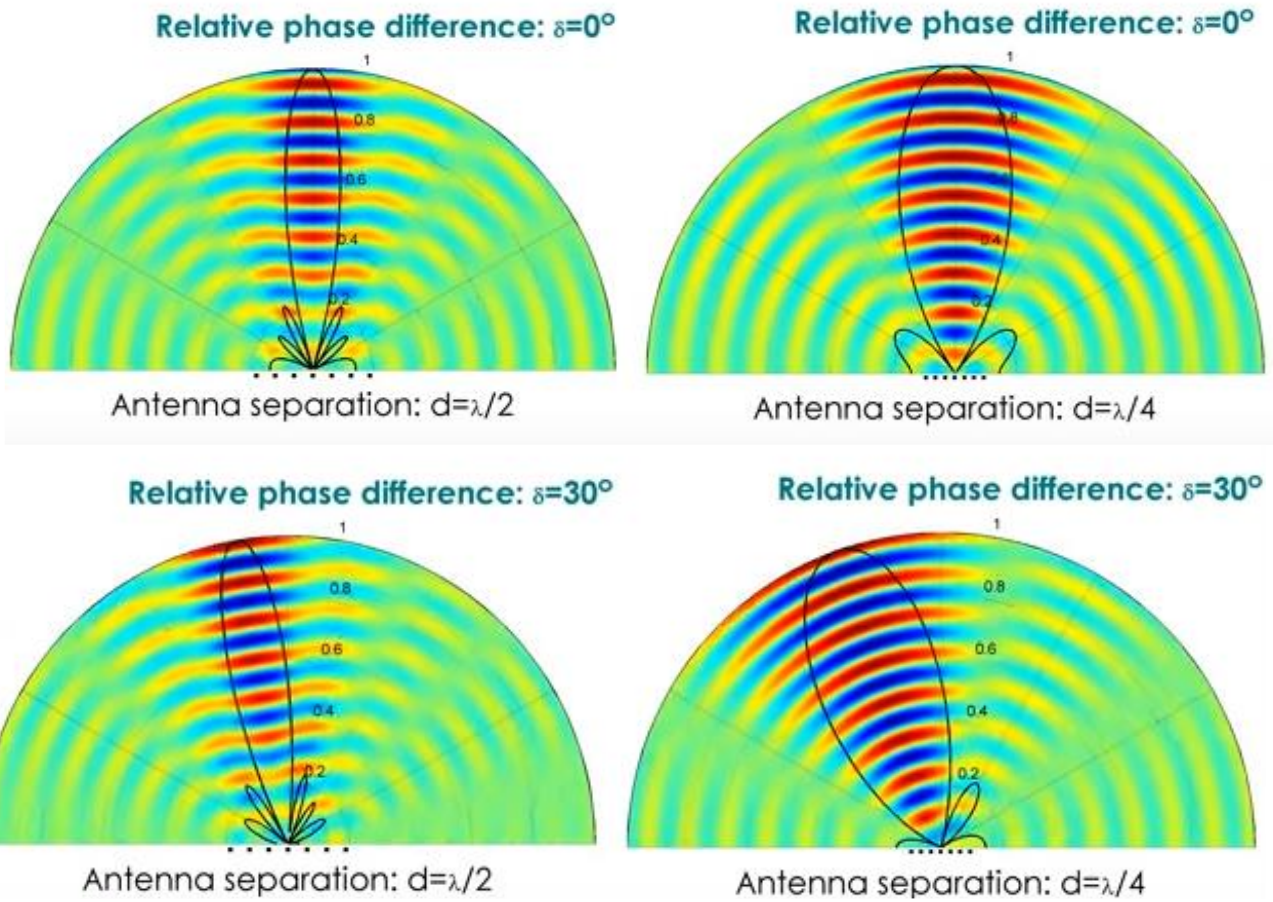
- Exploitation de plusieurs antennes en émission et en réception :

MIMO : Multiple Input Multiple Output, principe appelé multiplexage spatial

Beamforming



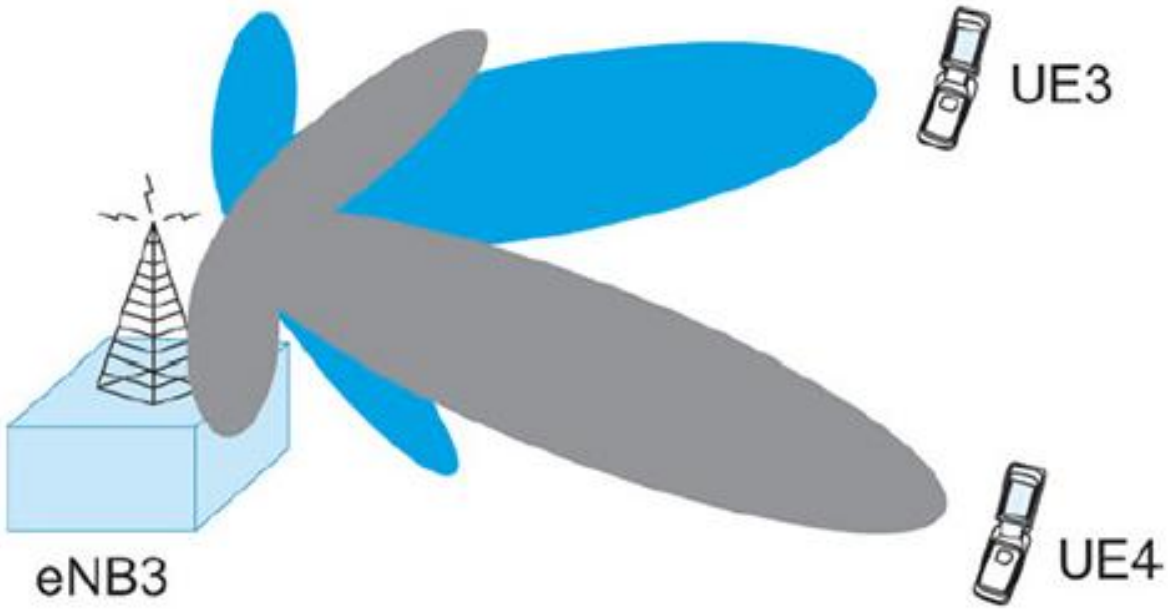
Beamforming



https://www.youtube.com/watch?v=VBFsisCjpBk

Beamforming

- Exemple d'utilisation de beamforming grâce au MIMO



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

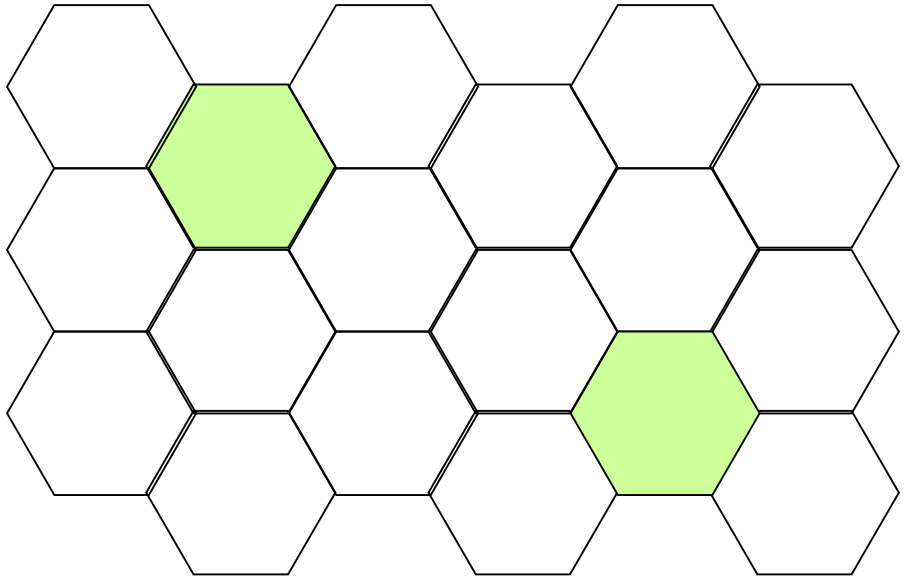
de taille variable :

  - 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)

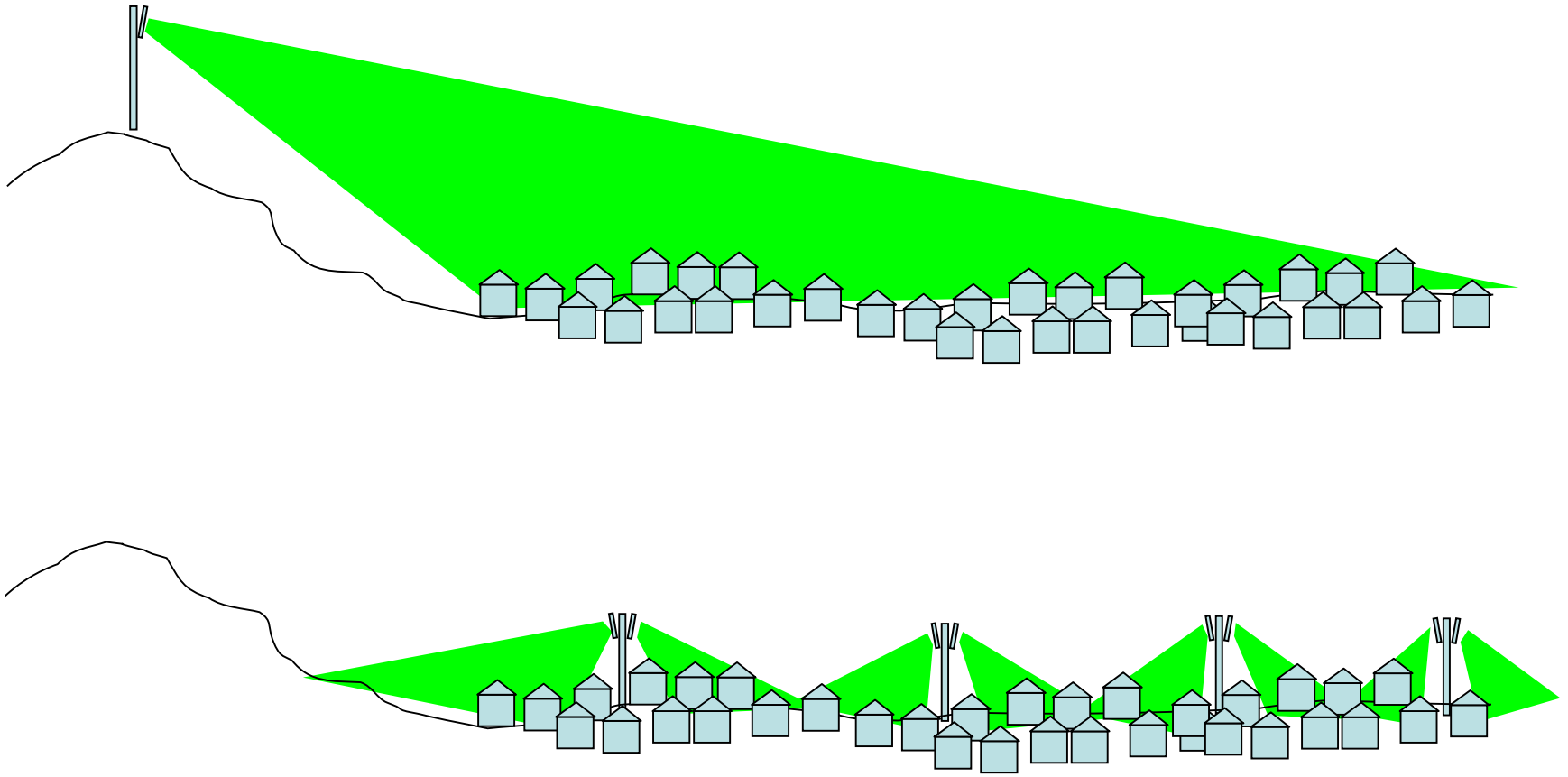
Organisation cellulaire

- Réutilisation de la même fréquence sur des zones géographiques différentes



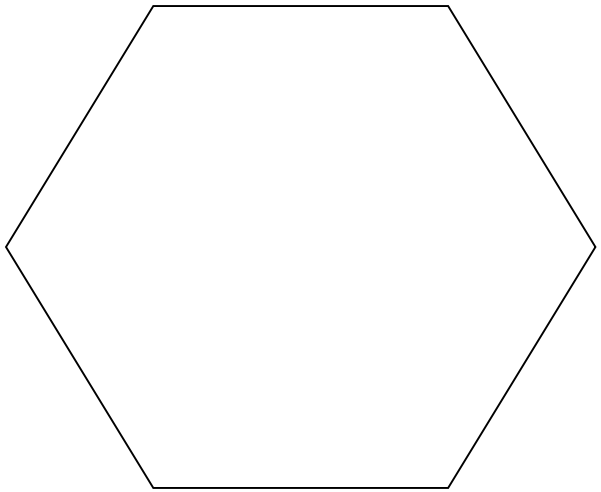
- Avantage : augmentation de la capacité
- Inconvénient : augmentation des interférences

Implantation des antennes

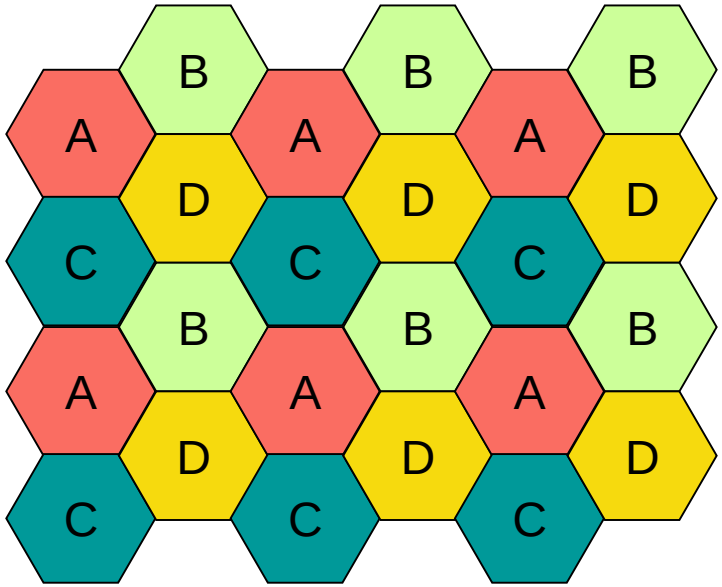


Exemple : couverture d'une zone

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

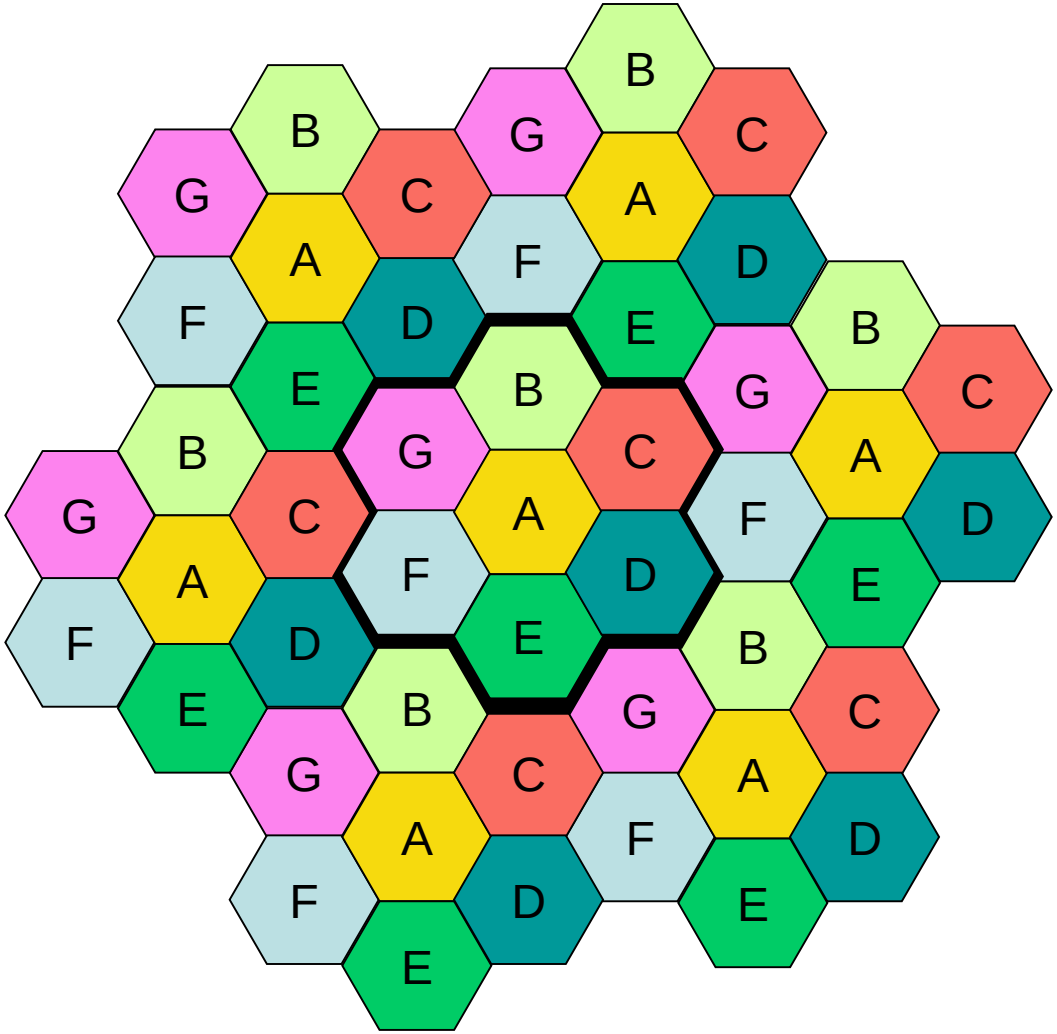
- Facteur de réutilisation

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

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

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

Protocole 802.11	date	Fréquence (GHz)	largeur de bande (MHz)	Débit binaire par flux MIMO (Mbit/s)	Nombre maximum de flux MIMO	Codage / Modulation	Portée Intérieur (mètres)	Portée Extérieur (mètres)
802.11-1997 (d'origine)	juin 1997	2,4	79 ou 22	1, 2 Mbit/s	NC	FHSS, DSSS	20 m	100 m
802.11a	sept 1999	5 3,7	20	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	NC	OFDM	35 m —	120 m 5 000 m
802.11b	sept 1999	2,4	22	1, 2, 5,5, 11 Mbit/s	1	DSSS	35 m	140 m
802.11g	juin 2003	2,4	20	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	1	DSSS, OFDM	38 m	140 m

Standards IEEE 802.11

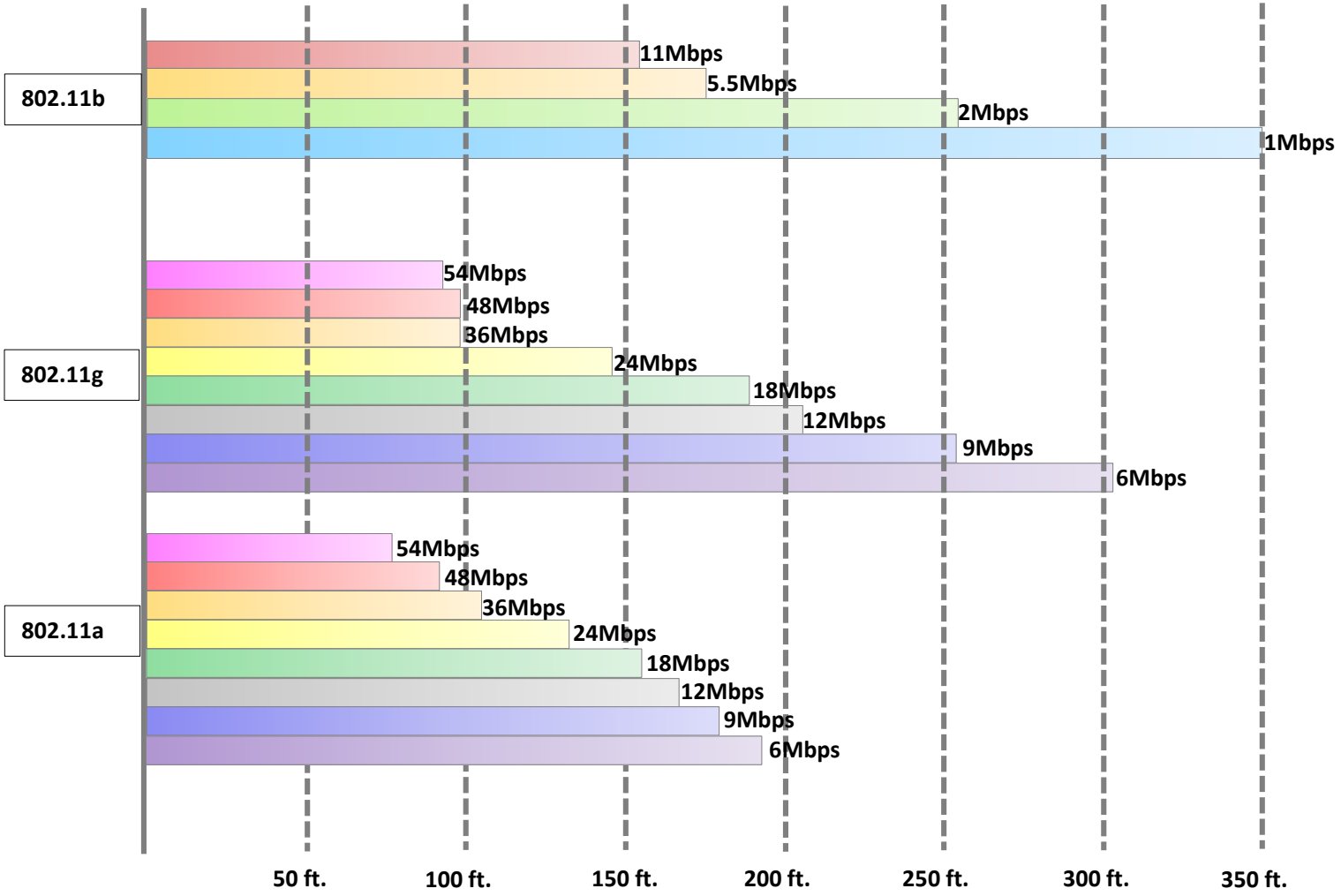
Protocole 802.11	date	Fréquence (GHz)	largeur de bande (MHz)	Débit binaire par flux MIMO (Mbit/s)	Nombre maximum de flux MIMO	Codage / Modulation	Portée Intérieur (mètres)	Portée Extérieur (mètres)
802.11n	oct 2009	2,4 / 5	20	7,2 à 72,2 Mbit/s (6,5 à 65)	4	OFDM	70 m (2,4 GHz)	250 m
			40	15 à 150 Mbit/s (13,5 à 135)			35 m (5 GHz)	250 m
802.11ac	déc 2013	5	20	7,2 à 96 Mbit/s (6,5 à 86,7)	8	OFDM	35 m	
			40	15 à 200 Mbit/s (13,5 à 80)			35 m	
			80	32,5 à 433 Mbit/s (29,2 à 390)				
			160	65 à 866 Mbit/s (58,5 à 780)			35 m	
							35 m	

Standards IEEE 802.11

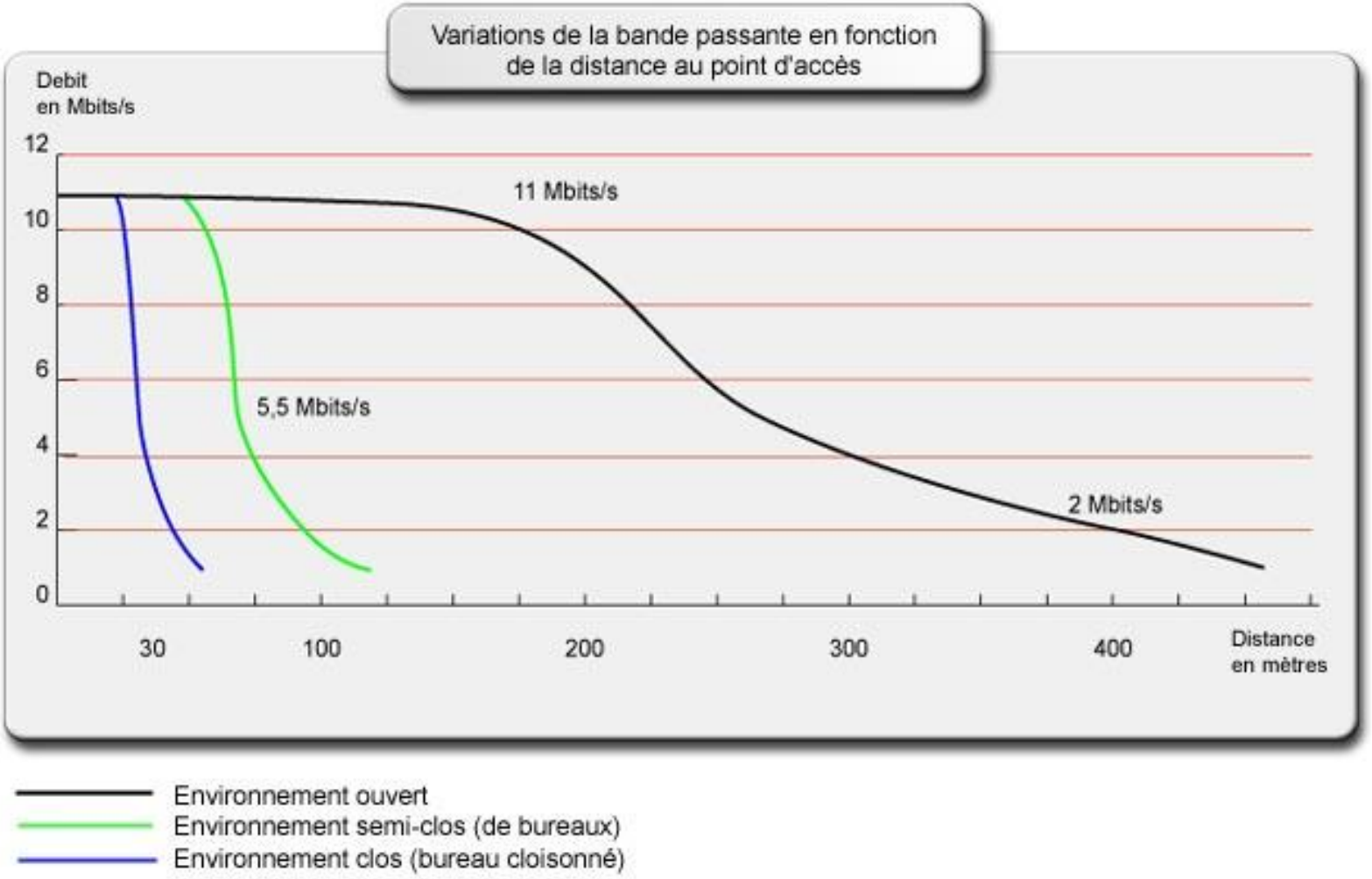
Protocole 802.11	date	Fréquence (GHz)	largeur de bande (MHz)	Débit binaire par flux MIMO (Mbit/s)	Nombre maximum de flux MIMO	Codage / Modulation	Portée Intérieur (mètres)	Portée Extérieur (mètres)
802.11ad	déc 2012	60	2,160	jusqu'à 6,75 Gbit/s	NC	OFDM ou simple porteuse	10 m	
802.11ah	est. 2016	0,9	1 à 8	0,6 à 8 Mbit/s	1, 2	OFDM	100 m	

Débits en fonction de la distance

(intérieur, bureaux ouverts)



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.

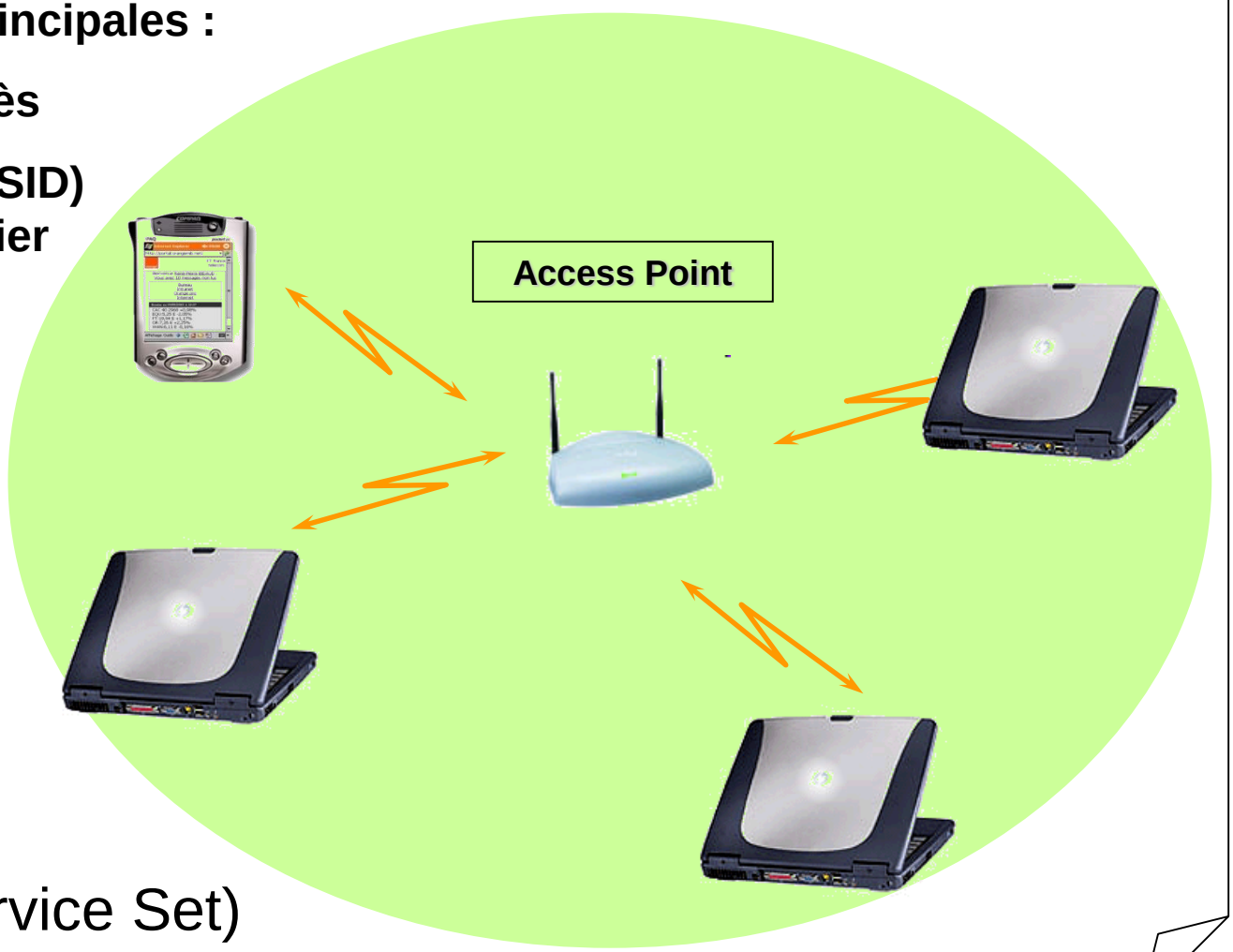
IEEE 802.11 : Architecture

- 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

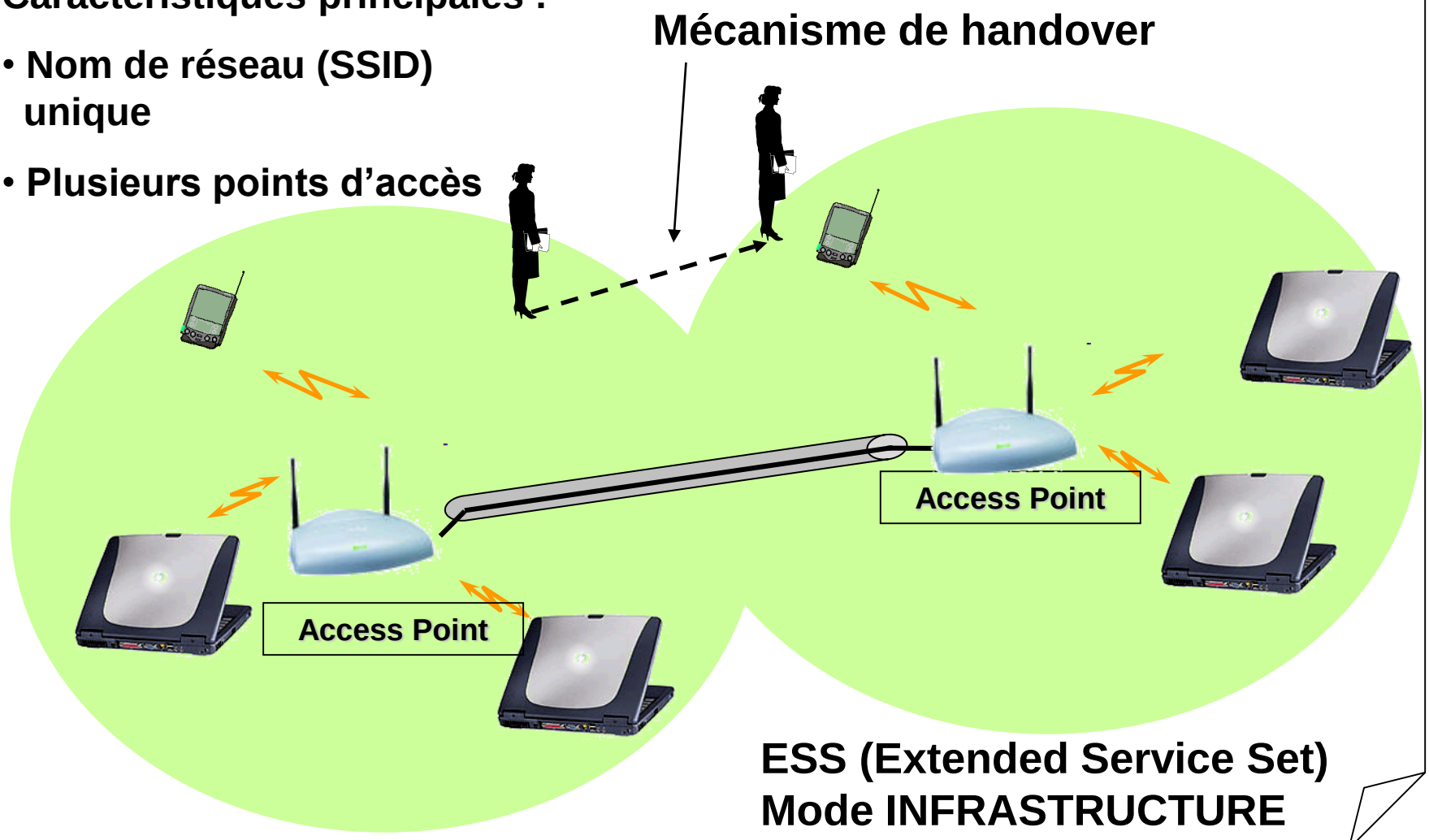


BSS (Basic Service Set)

IEEE 802.11 : Architecture ESS et handover

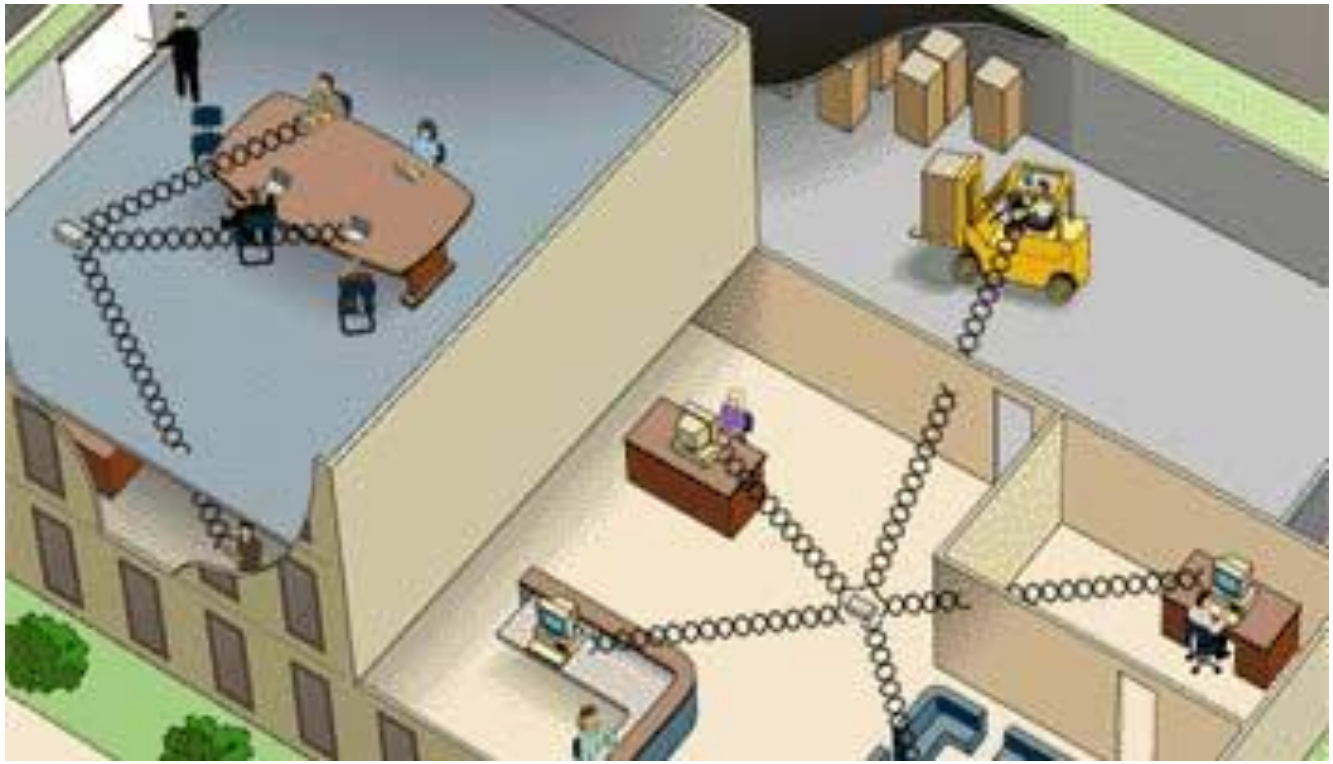
Caractéristiques principales :

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



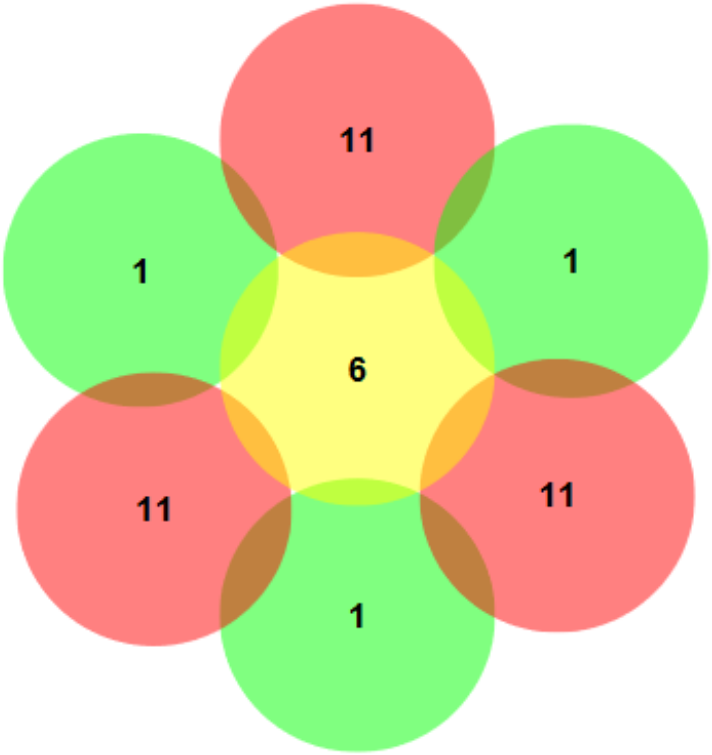
ESS (Extended Service Set)
Mode INFRASTRUCTURE

IEEE 802.11 : Architecture ESS

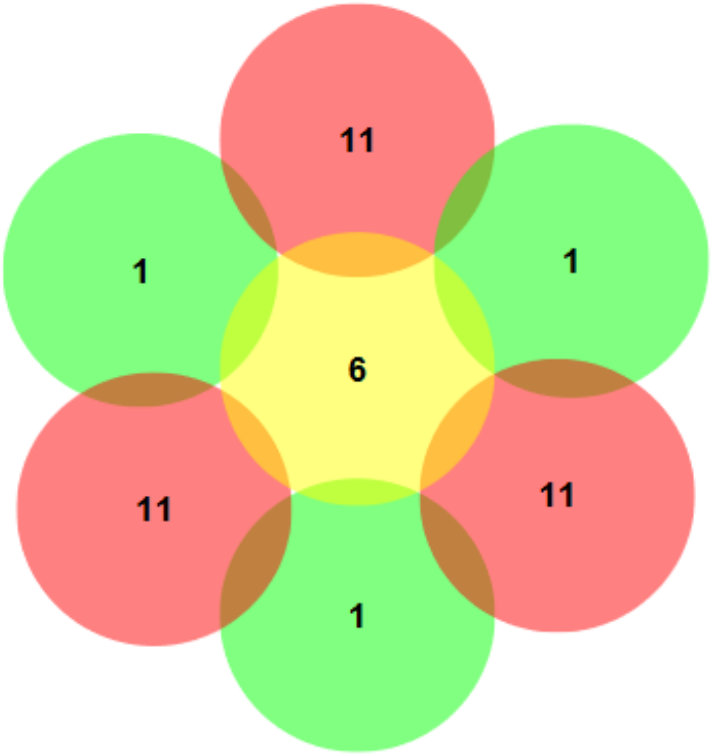


IEEE 802.11 : Architecture ESS

- Disposition des bornes sans recouvrement



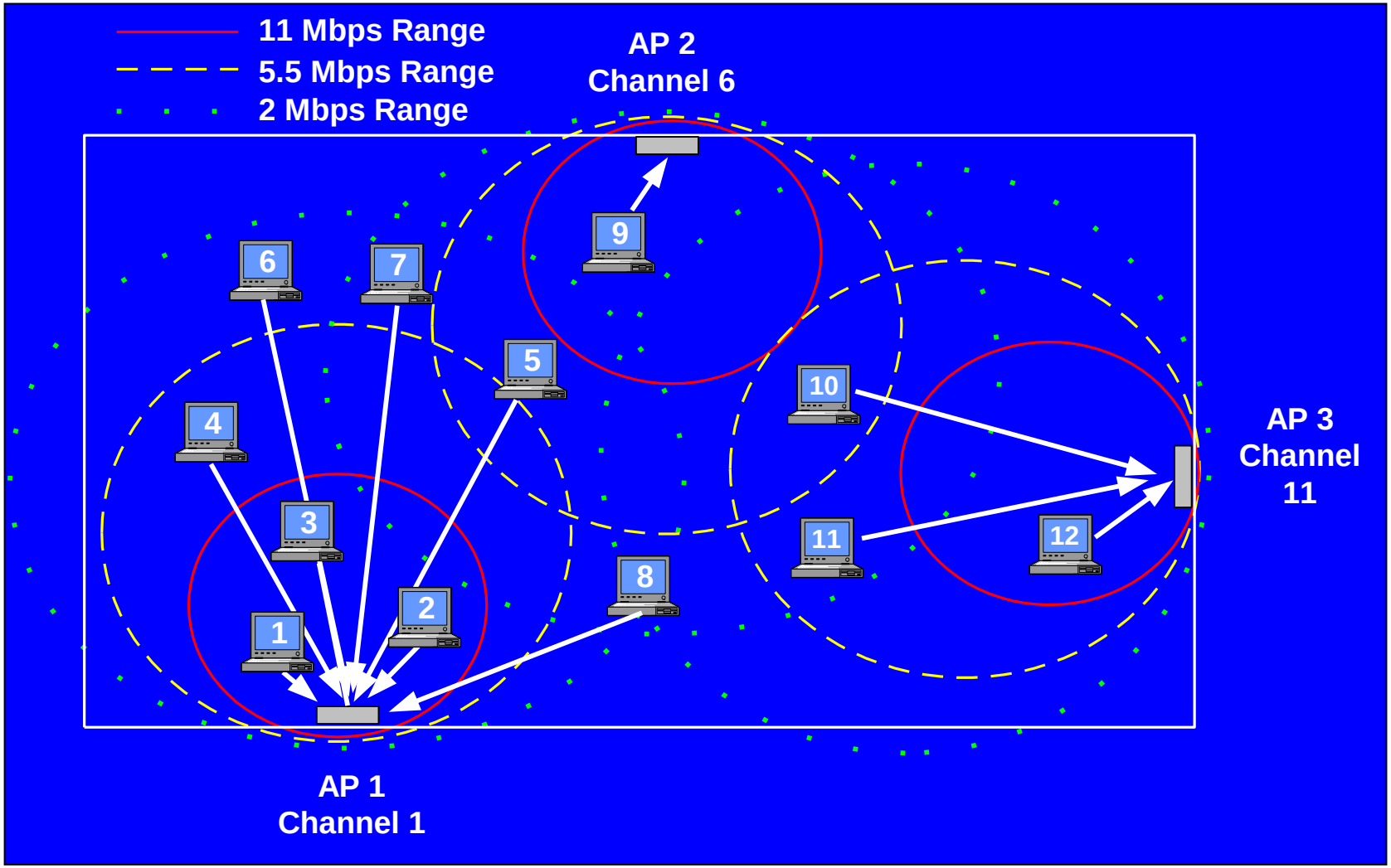
IEEE 802.11 : Architecture ESS



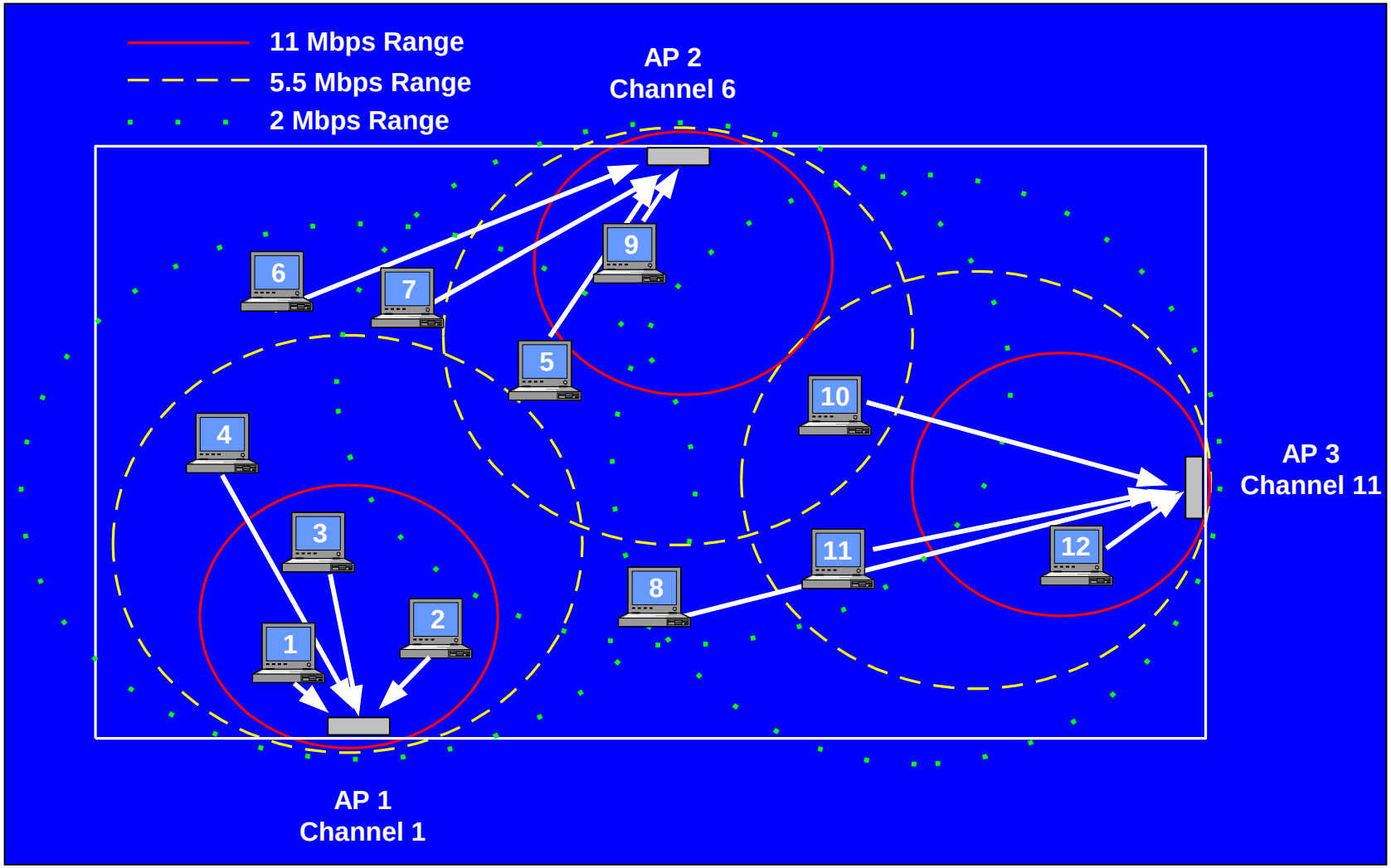
IEEE 802.11 : Architecture ESS

- 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**



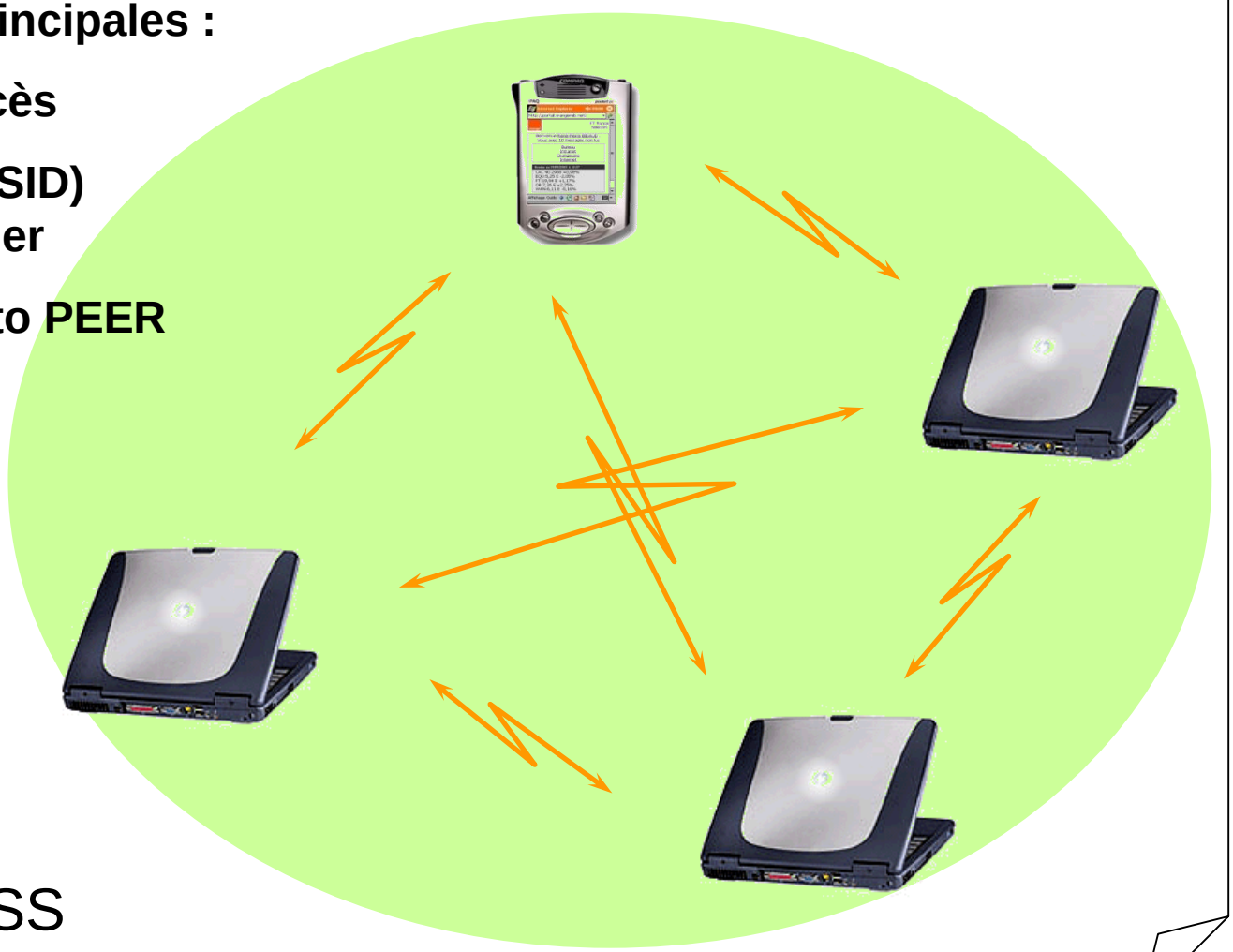
Répartition dynamique de charge : **après**



IEEE 802.11 : Architecture IBSS (Mode ad'hoc)

Caractéristiques principales :

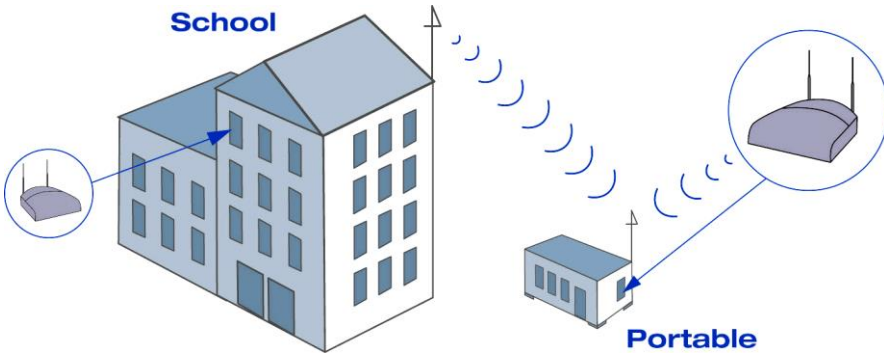
- **Pas de point d'accès**
- **Nom de réseau (SSID)**
  Service Set Identifier
- **Topologie : PEER to PEER**



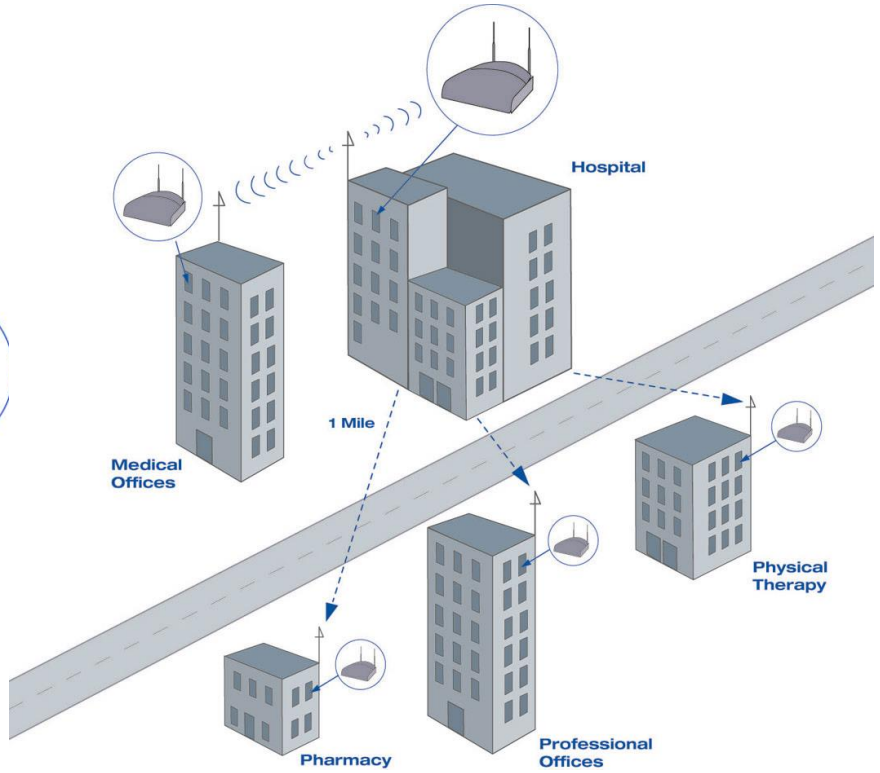
Independant BSS

Pont radio

Point à point



Point à multipoints

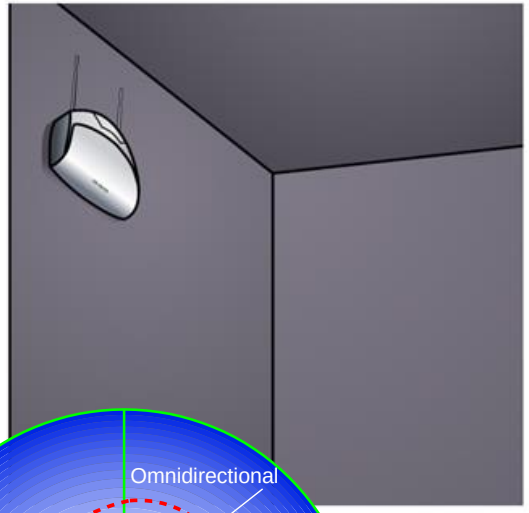


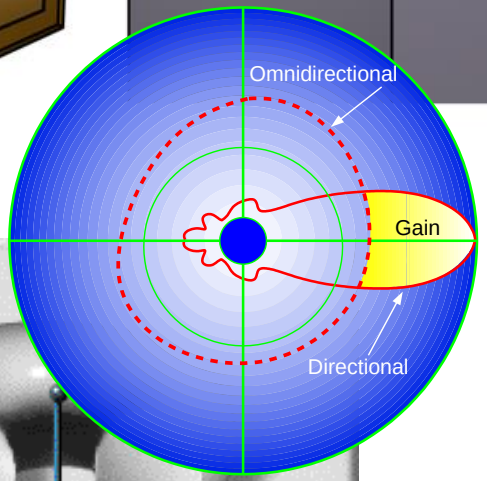
Matériel

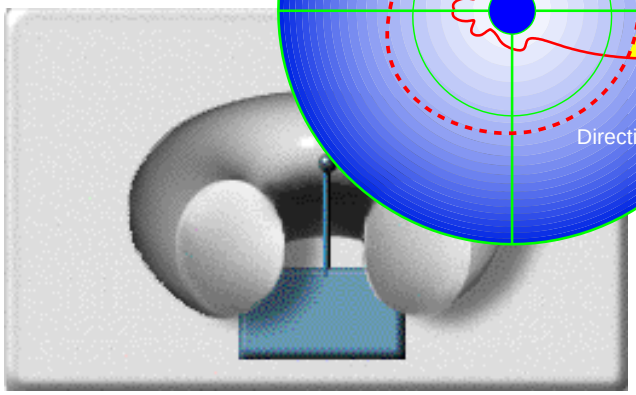
- Éléments actifs
  - Point d’accès
  - Bridge
  - Point to Multipoint
  - AP Client

- Éléments passifs
  - cartes clientes (PCMCIA, PCI, USB)
  - antennes

Antennes : orientation

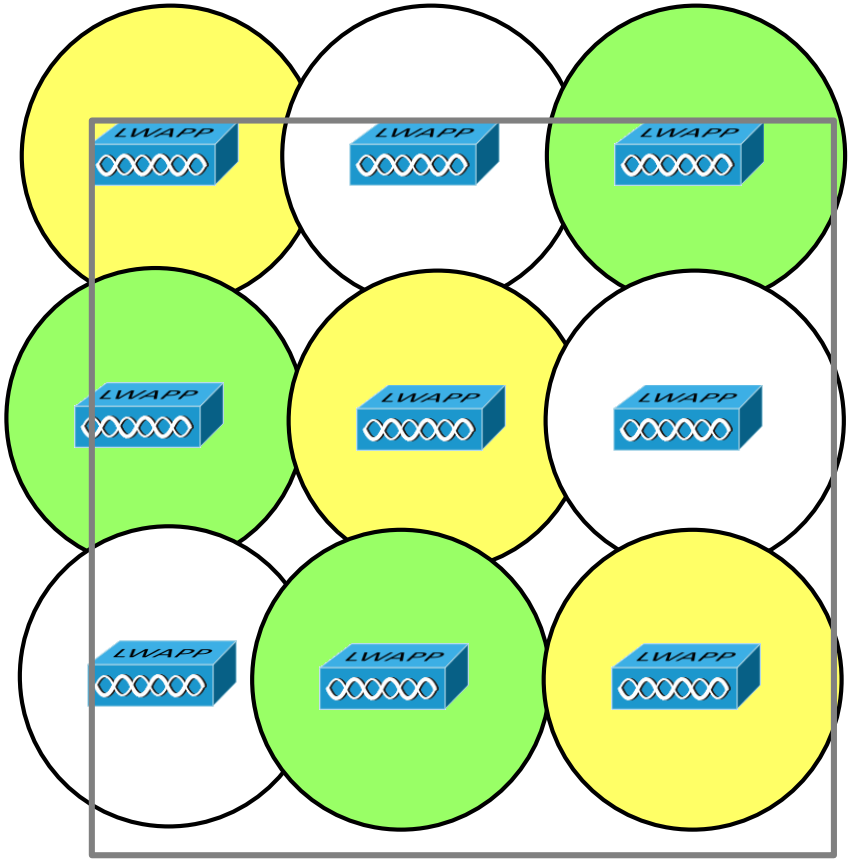






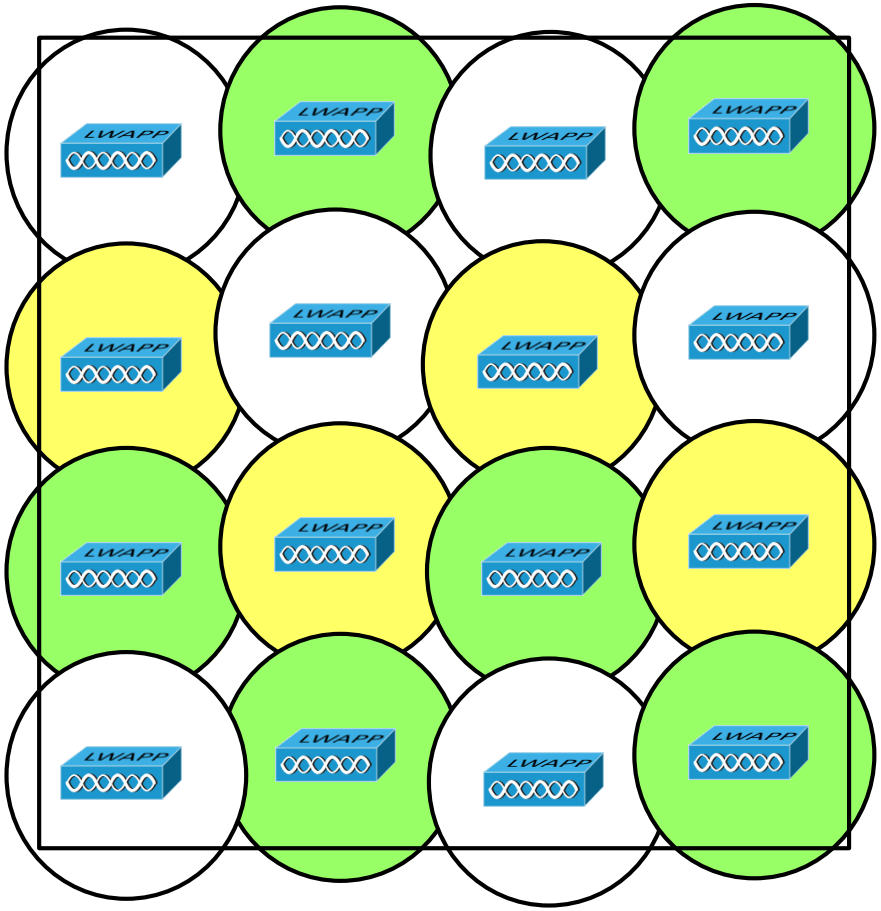
Couverture

- Exemple de base



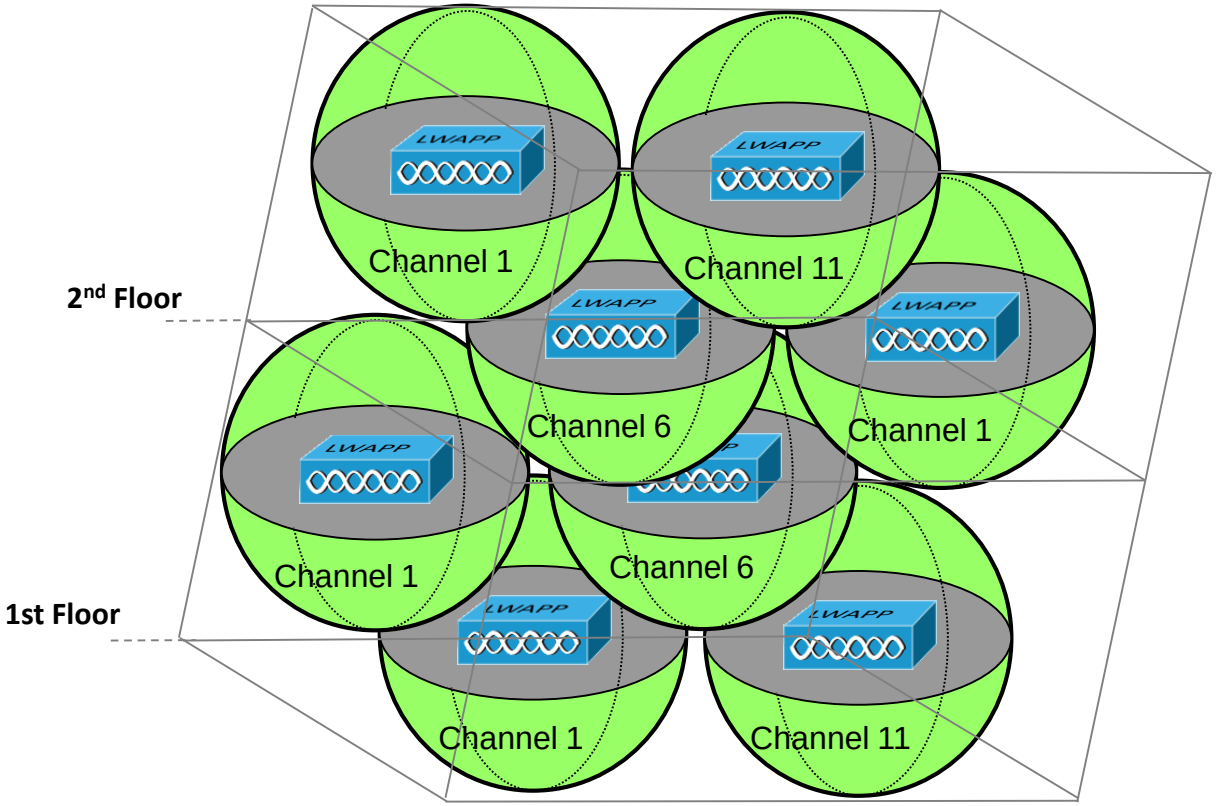
Couverture

- Couverture plus dense



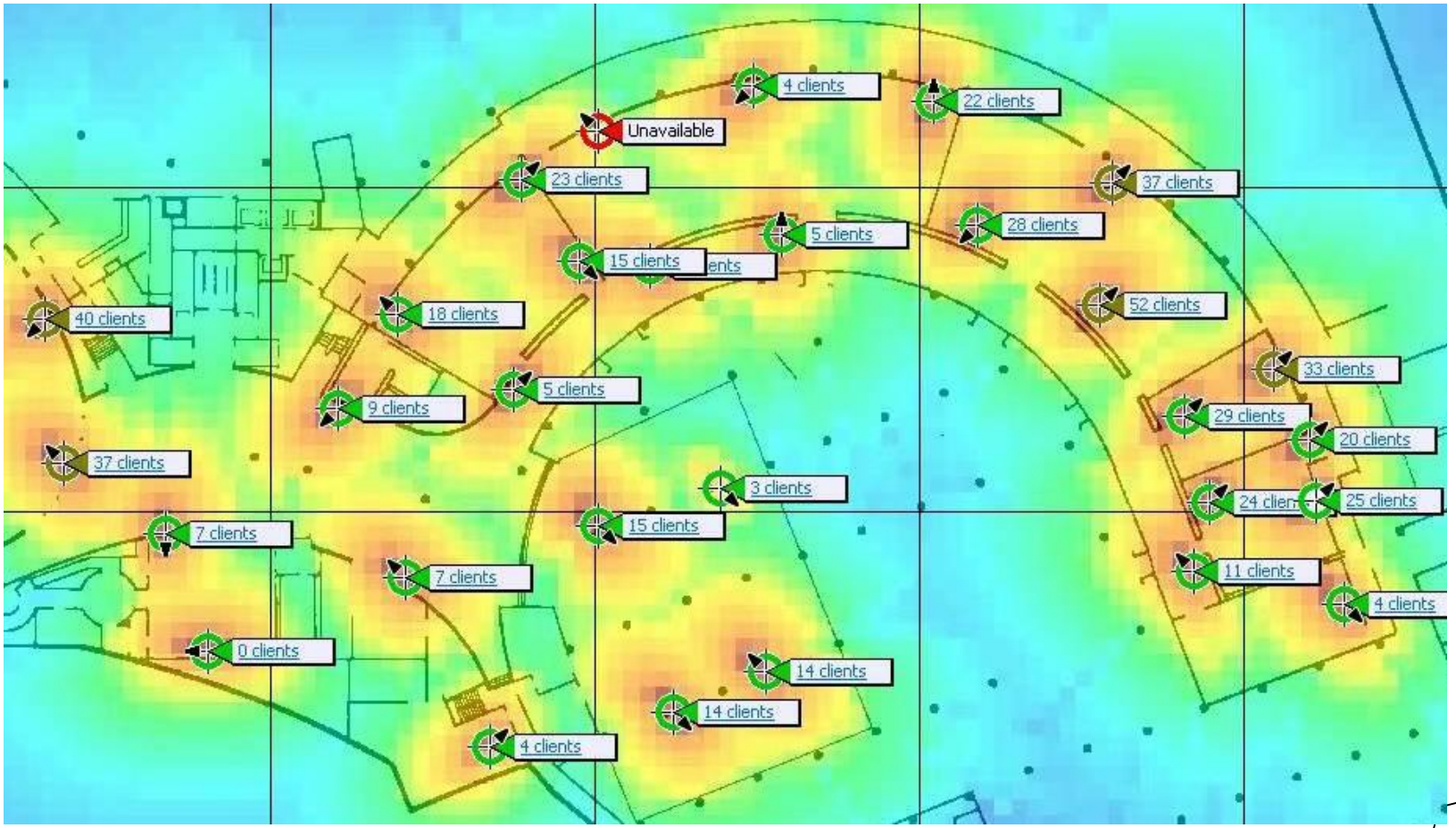
Couverture

- Couverture sur plusieurs étages (3D)



Couverture

- Etude de couverture : HeatMap



IEEE 802.11

Couche physique

802.11 Modèle OSI

<table>
<tr><td rowspan="2">Couche liaison de données</td><td colspan="4">LLC 802.2</td></tr>
<tr><td colspan="4">MAC 802.11, sécurité, etc …</td></tr>
<tr><td>Couche physique</td><td>FHSS</td><td>DSSS</td><td>IR</td><td>OFDM</td></tr>
</table>

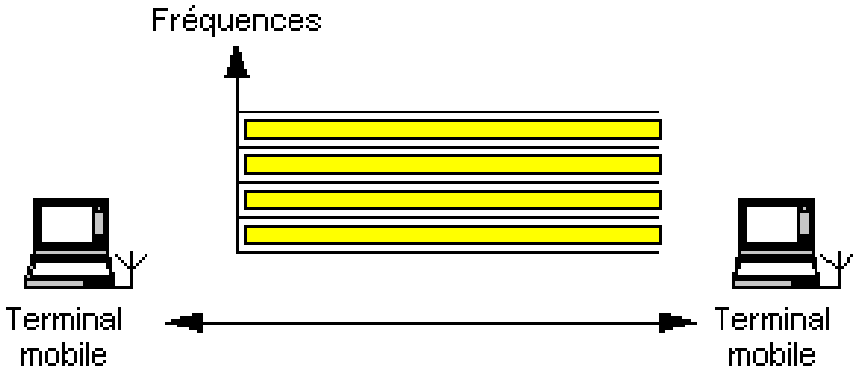
- FHSS : étalement de spectre par saut de fréquence
- DSSS : étalement de spectre en séquence directe
- IR : InfraRouge
- OFDM : Multiplexage en fréquences

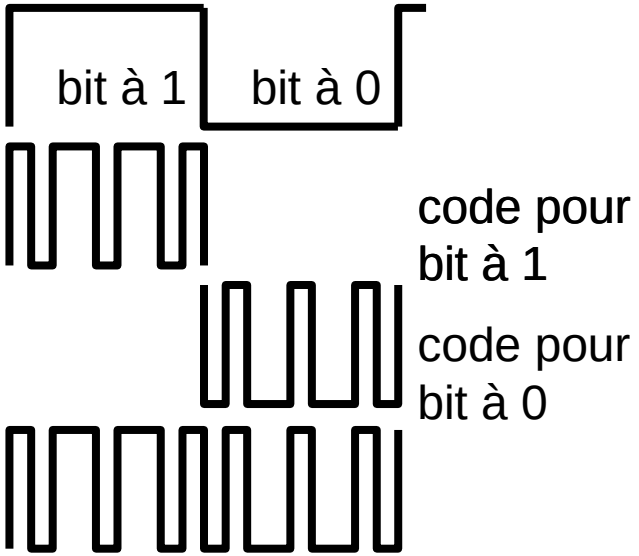
FHSS : étalement de spectre par saut de fréquence

- 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.



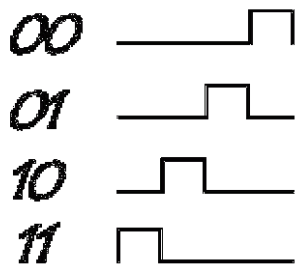


Étalement de spectre : Comparatif

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

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

- 802.11a/g utilise OFDM avec un système de 52 porteuses (appelées parfois sous-porteuses)
- Modulation par BPSK ou QPSK.
- Etalement spectral OFDM : distribution des données sur les 52 porteuses

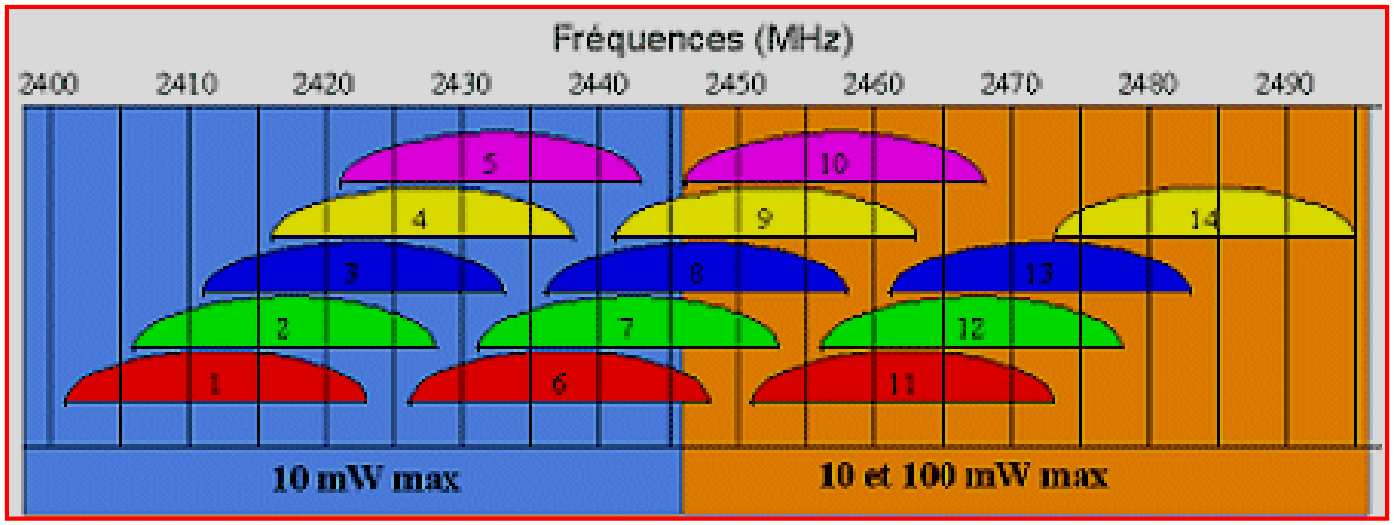
Types de modulation

- PSK (Modulation de phase)
- QPSK (Modulation de phase en quadrature)
- CCK (Complementary Code Keying)
  Symboles de n 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)

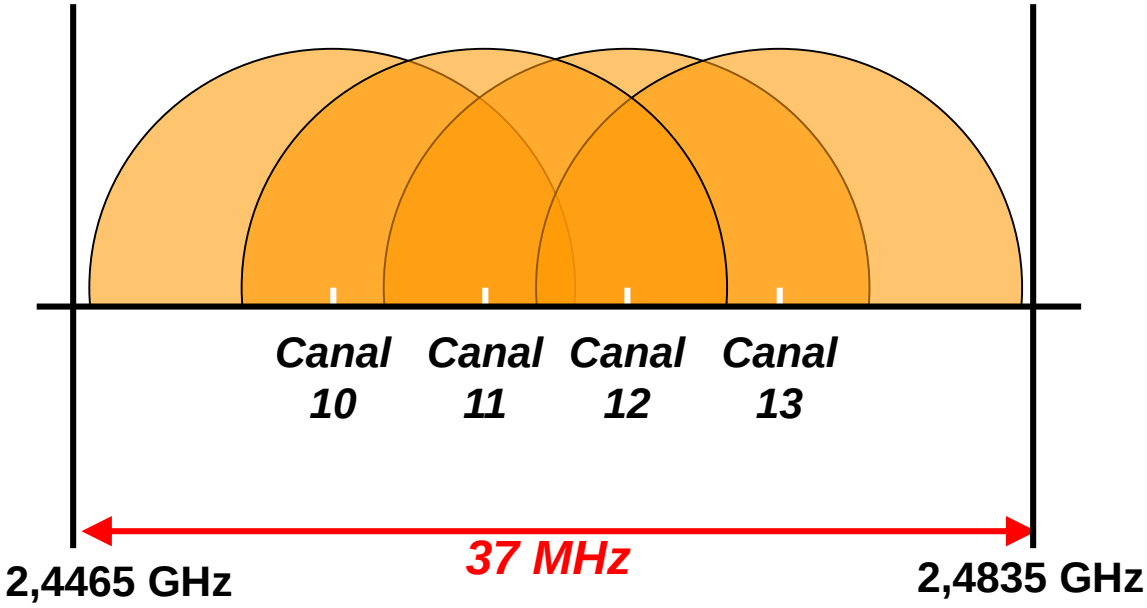
- Bande ISM
  - Bande divisée en 14 canaux de 20 MHz
  - Problème de recouvrement
  - Superposition de 3 réseaux au sein d'un même espace
  - Largeur de bande 83 MHZ



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

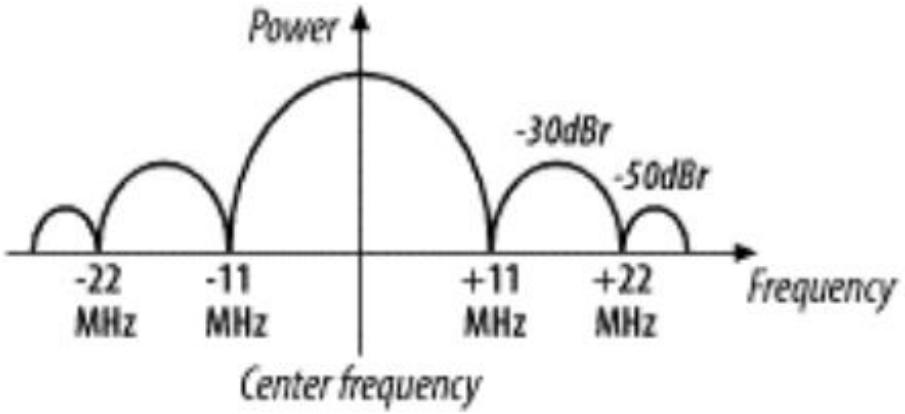
Bande ISM

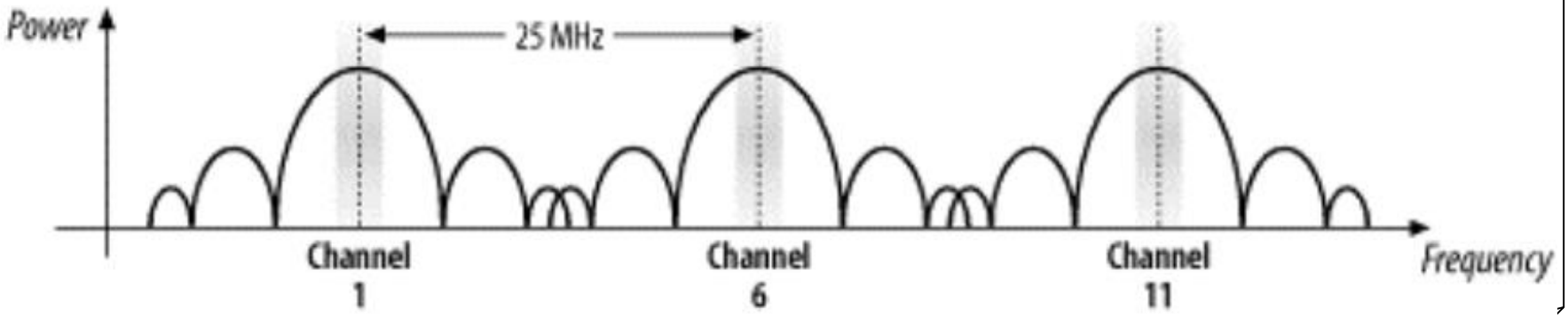
"Pays"	États-unis	Europe	Japon
Nombres de sous-canaux utilisés	1 à 11	1 à 13	14



802.11 DS

- Répartition de l'énergie spectrale





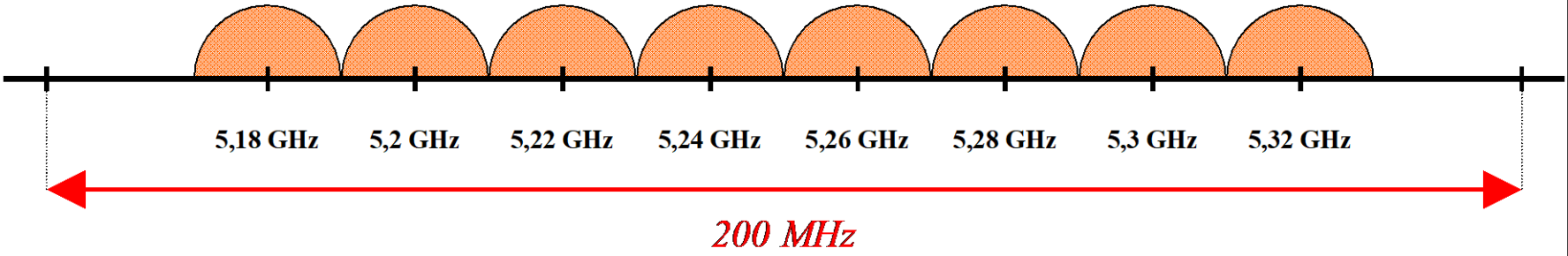
802.11b - Portée

- 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

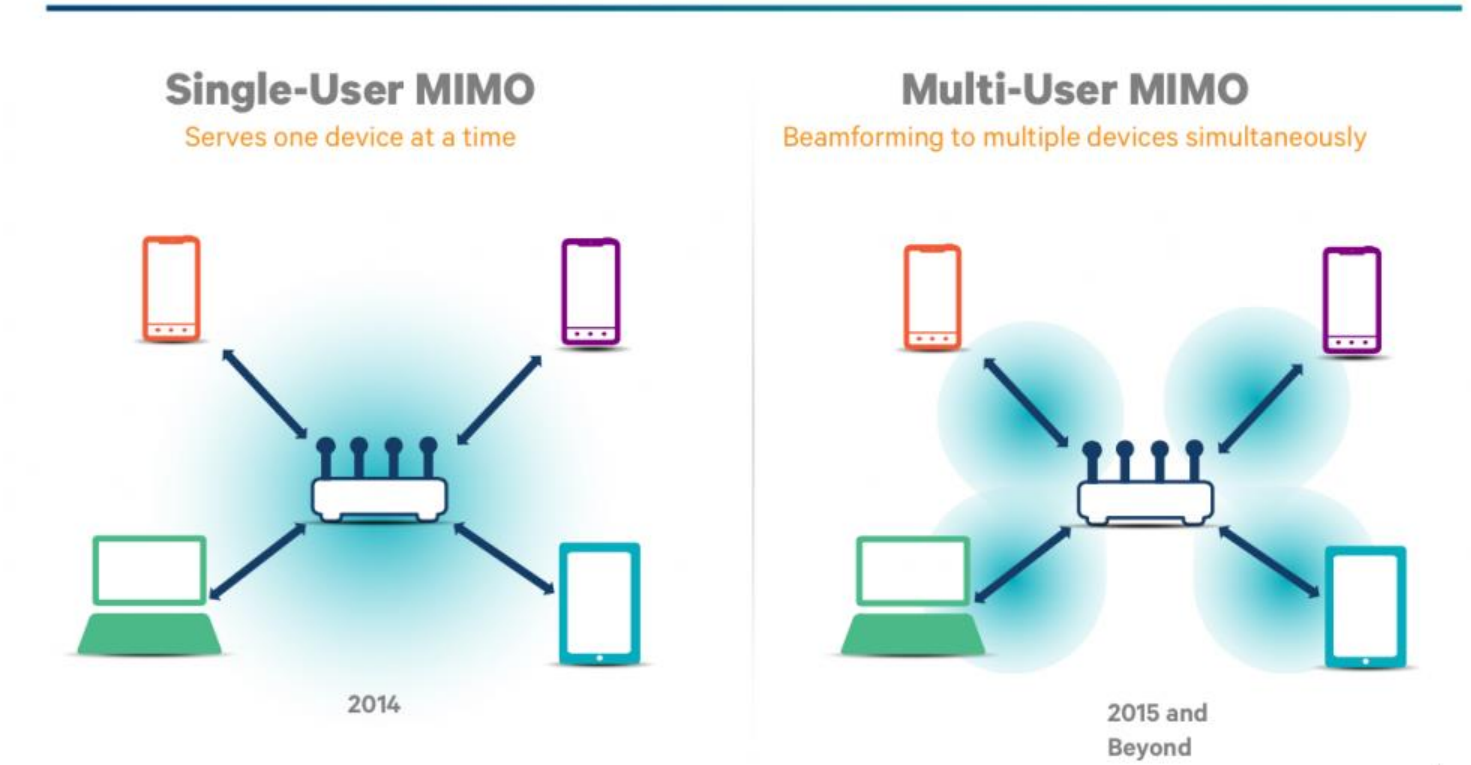
- La bande ISM est de plus en plus saturée (802.11b, 802.11g, Bluetooth, etc.)

802.11n

- Introduit le MIMO (*Multiple-Input Multiple-Output)*, qui utilise plusieurs antennes d'émission et de reception pour augmenter le debit ("smart antennas").
- Peut avoir jusqu'à 8 antennes. La majorité n'utilise que 4 antennes au maximum
- Avec 4 antennes, 2 peuvent servir en émission, 2 en reception simutanément
- Permet un débit bien supérieur à 802.11a/b/g

802.11 ac

- MU-MIMO (au lieu de SU-MIMO)
  Multi-Utilisateur, Multiple-Input, Multiple-Output



802.11 ac

- MU-MIMO

Utilisation du Beamforming

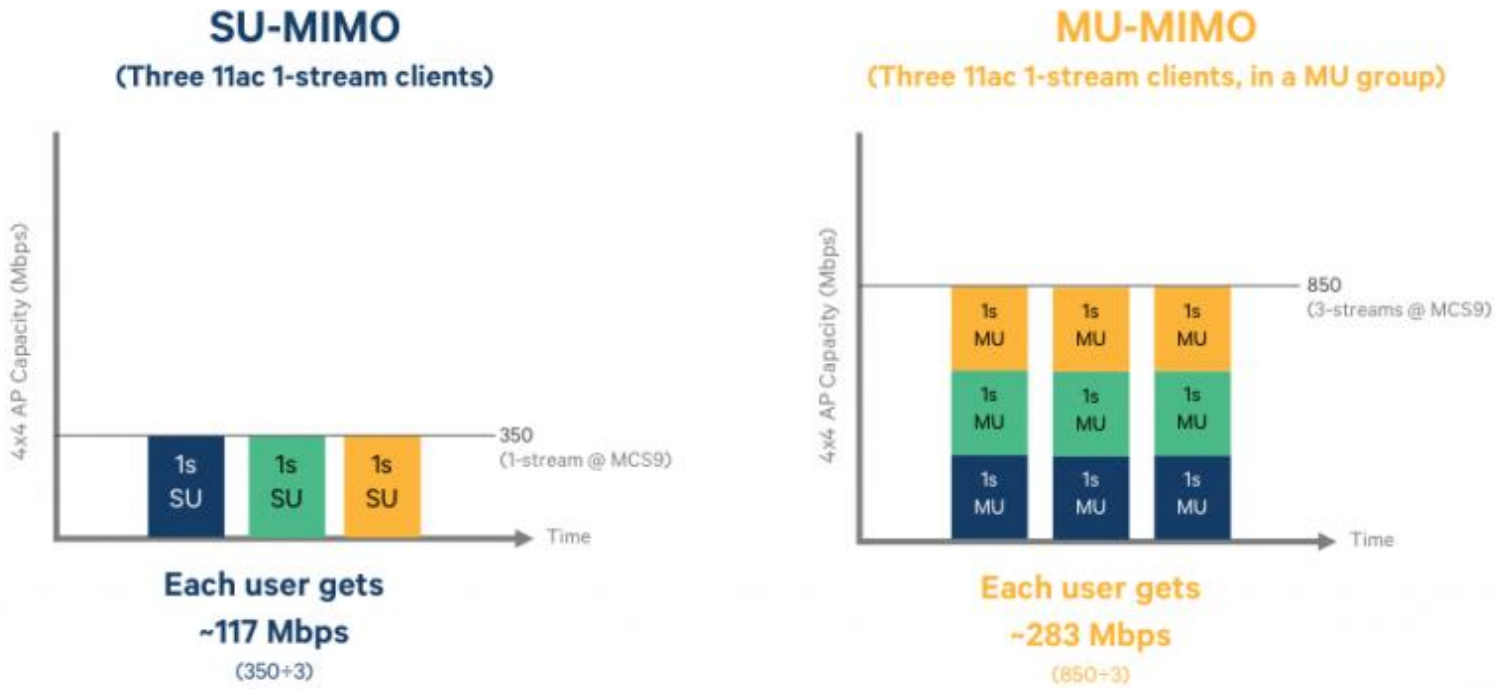
Les terminaux du même groupe (4 maxi) recoivent en parallèle.

Au-delà de 4, plusieurs groupes seront créés (64 maxi), utilisation du TDMA pour les groupes.

802.11 ac

- MU-MIMO

Performances jusqu'à 2 à 3 fois supérieures.



802.11 ac

802.11ac Wave 2 Max Data Rate at 80 & 160 MHz

BW (MHz)	# Spatial Streams	Modulation Type	PHY Rate (Mbps)	MAC Thru-put (Mbps)*
80	1	64	325	189
80	1	256	390	215
80	1	256	433	280
80	2	64	650	423
80	2	256	780	507
80	2	256	867	564
80	3	64	975	634
80	3	256	1170	761
80	3	256	1300	845

BW (MHz)	# Spatial Streams	Modulation Type	PHY Rate (Mbps)	MAC Thru-put (Mbps)*
160	1	64	650	422
160	1	256	780	507
160	1	256	867	563
160	2	64	1300	845
160	2	256	1560	1014
160	2	256	1732	1126
160	3	64	1950	1268
160	3	256	2340	1521
160	3	256	2600	1690

- With 802.11ac Wave 2 we have the ability to exceed 1 Gbps of uplink traffic

1 actively serving 5 GHz radio operating at **160 MHz**

e.g. 2SS at 256 QAM = 1126 Mbps

e.g. 3SS at 256 QAM = 1521 Mbps

2 actively serving 5 GHz radio's at **80 MHz** wide

e.g. 3SS at 256 QAM = 780 Mbps x 2 = 1560 Mbps

e.g. 2SS at 256 QAM = 520 Mbps x 2 = 1040 Mbps

*Assumes 65% MAC efficiency

MCS: Modulation and Coding Scheme

http://www.mcsindex.com

MCS Value Achieved by Clients at Various Signal to Noise Ratio Levels (SNR)

Protocol	Channel	1	2	3	4	5	6	7	8	9	10
802.11b	20MHz	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1
802.11a/g	20MHz	None	MCS 0	MCS 0	MCS 1	MCS 2	MCS 2	MCS 2	MCS 2	MCS 3	MCS 3
802.11n	20MHz	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2
802.11n	40MHz	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1
802.11ac	20MHz	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2
802.11ac	40MHz	None	None	None	None	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1
802.11ac	80MHz	None	None	None	None	None	None	None	MCS 0	MCS 0	MCS 0
802.11ac	160MHz	None	None	None	None	None	None	None	None	None	None

Modulation Key
None = Grey
BPSK = Red
QPSK = Orange
16-QAM = Yellow
64-QAM = Blue
256-QAM = Green

	SNR in dB	11	12	13	14	15	16	17	18	19	20
802.11b	20MHz	MCS 2	MCS 2	MCS 2	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 4	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 5	MCS 6	MCS 6	MCS 7
802.11n	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6
802.11n	40MHz	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4
802.11ac	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6
802.11ac	40MHz	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4
802.11ac	80MHz	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3	MCS 3	MCS 3	MCS 3
802.11ac	160MHz	MCS 0	MCS 0	MCS 0	MCS 1	MCS 1	MCS 1	MCS 1	MCS 2	MCS 2	MCS 3

802.11 Type Key
802.11b
802.11ag
802.11n
802.11ac

	SNR in dB	21	22	23	24	25	26	27	28	29	30
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8
802.11ac	40MHz	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7
802.11ac	80MHz	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6	MCS 6	MCS 6	MCS 6	MCS 6
802.11ac	160MHz	MCS 3	MCS 3	MCS 3	MCS 4	MCS 4	MCS 4	MCS 5	MCS 5	MCS 6	MCS 6

	SNR in dB	31	32	33	34	35	36	37	38	39	40
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	40MHz	MCS 7	MCS 8	MCS 8	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	80MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	160MHz	MCS 6	MCS 6	MCS 6	MCS 7	MCS 7	MCS 7	MCS 7	MCS 8	MCS 8	MCS 9

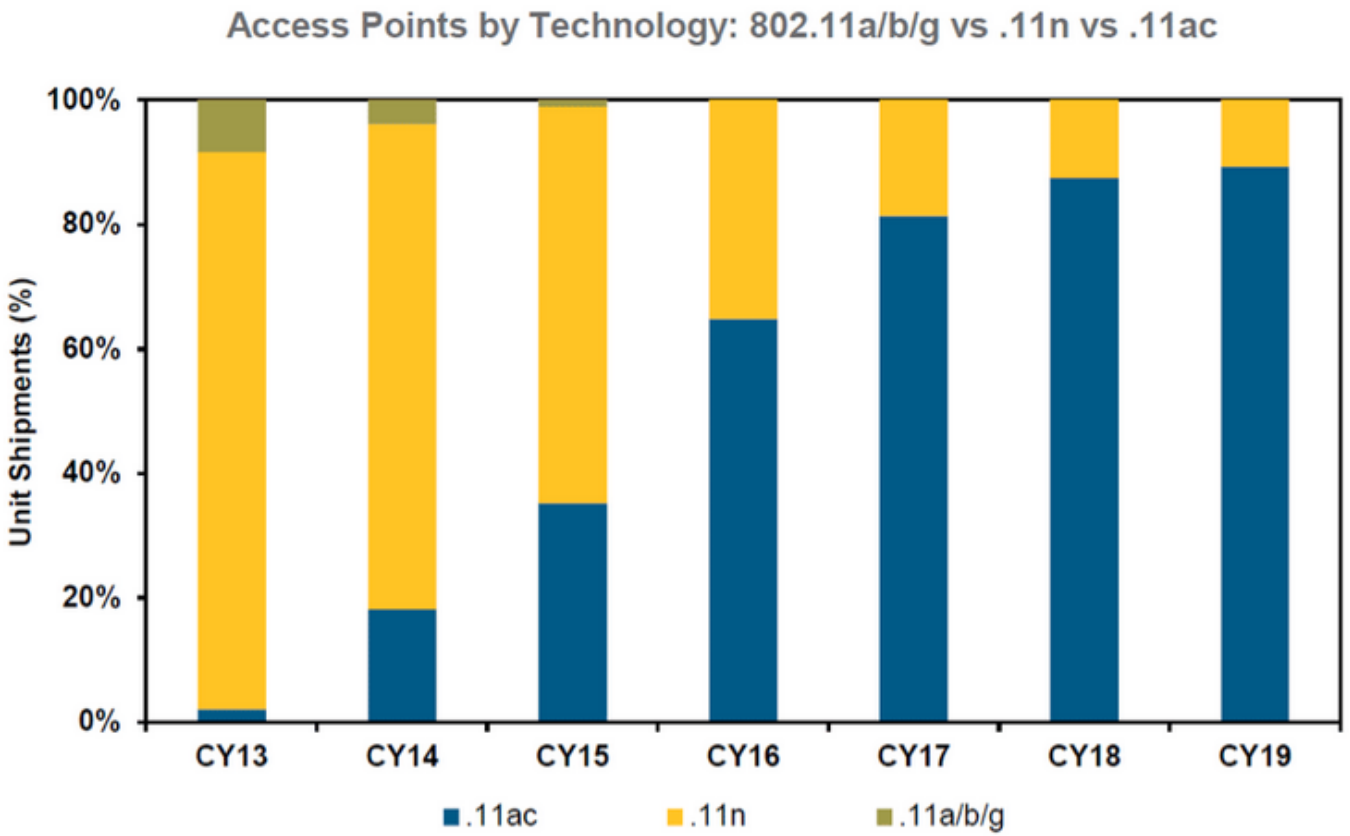
	SNR in dB	41	42	43	44	45	46	47	48	49	50
802.11b	20MHz	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3	MCS 3
802.11a/g	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	20MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11n	40MHz	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7	MCS 7
802.11ac	20MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	40MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	80MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9
802.11ac	160MHz	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9	MCS 9

802.11n											802.11ac
HT MCS Index	Spatial Streams	Modulation & Coding	Data Rate GI = 800ns 20MHz	Data Rate SGI = 400ns 20MHz	Data Rate GI = 800ns 40MHz	Data Rate SGI = 400ns 40MHz	Data Rate GI = 800ns 80MHz	Data Rate SGI = 400ns 80MHz	Data Rate GI = 800ns 160MHz	Data Rate SGI = 400ns 160MHz	VHT MCS Index
0	1	BPSK 1/2	6.5	7.2	13.5	15	29.3	32.5	58.5	65	0
1	1	QPSK 1/2	13	14.4	27	30	58.5	65	117	130	1
2	1	QPSK 3/4	19.5	21.7	40.5	45	87.8	97.5	175.5	195	2
3	1	16-QAM 1/2	26	28.9	54	60	117	130	234	260	3
4	1	16-QAM 3/4	39	43.3	81	90	175.5	195	351	390	4
5	1	64-QAM 2/3	52	57.8	108	120	234	260	468	520	5
6	1	64-QAM 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	6
7	1	64-QAM 5/6	65	72.2	135	150	292.5	325	585	650	7
	1	256-QAM 3/4	78	86.7	162	180	351	390	702	780	8
	1	256-QAM 5/6	n/a	n/a	180	200	390	433.3	780	866.7	9
8	2	BPSK 1/2	13	14.4	27	30	58.5	65	117	130	0
9	2	QPSK 1/2	26	28.9	54	60	117	130	234	260	1
10	2	QPSK 3/4	39	43.3	81	90	175.5	195	351	390	2
11	2	16-QAM 1/2	52	57.8	108	120	234	260	468	520	3
12	2	16-QAM 3/4	78	86.7	162	180	351	390	702	780	4
13	2	64-QAM 2/3	104	115.6	216	240	468	520	936	1040	5
14	2	64-QAM 3/4	117	130.3	243	270	526.5	585	1053	1170	6
15	2	64-QAM 5/6	130	144.4	270	300	585	650	1170	1300	7
	2	256-QAM 3/4	156	173.3	324	360	702	780	1404	1560	8
	2	256-QAM 5/6	n/a	n/a	360	400	780	866.7	1560	1733.3	9
16	3	BPSK 1/2	19.5	21.7	40.5	45	87.8	97.5	175.5	195	0
17	3	QPSK 1/2	39	43.3	81	90	175.5	195	351	390	1
18	3	QPSK 3/4	58.5	65	121.5	135	263.3	292.5	526.5	585	2
19	3	16-QAM 1/2	78	86.7	162	180	351	390	702	780	3
20	3	16-QAM 3/4	117	130	243	270	526.5	585	1053	1170	4
21	3	64-QAM 2/3	156	173.3	324	360	702	780	1404	1560	5
22	3	64-QAM 3/4	175.5	195	364.5	405	n/a	n/a	1579.5	1755	6
23	3	64-QAM 5/6	195	216.7	405	450	877.5	975	1755	1950	7

802.11n												802.11ac
HT MCS Index	Spatial Streams	Modulation & Coding	Data Rate GI = 800ns 20MHz	Data Rate SGI = 400ns 20MHz	Data Rate GI = 800ns 40MHz	Data Rate SGI = 400ns 40MHz	Data Rate GI = 800ns 80MHz	Data Rate SGI = 400ns 80MHz	Data Rate GI = 800ns 160MHz	Data Rate SGI = 400ns 160MHz	VHT MCS Index
	3	256-QAM 3/4	234	260	486	540	1053	1170	2106	2340	8
	3	256-QAM 5/6	260	288.9	540	600	1170	1300	n/a	n/a	9
24	4	BPSK 1/2	26	28.9	54	60	117	130	234	260	0
25	4	QPSK 1/2	52	57.8	108	120	234	260	468	520	1
26	4	QPSK 3/4	78	86.7	162	180	351	390	702	780	2
27	4	16-QAM 1/2	104	115.6	216	240	468	520	936	1040	3
28	4	16-QAM 3/4	156	173.3	324	360	702	780	1404	1560	4
29	4	64-QAM 2/3	208	231.1	432	480	936	1040	1872	2080	5
30	4	64-QAM 3/4	234	260	486	540	1053	1170	2106	2340	6
31	4	64-QAM 5/6	260	288.9	540	600	1170	1300	2340	2600	7
	4	256-QAM 3/4	312	346.7	648	720	1404	1560	2808	3120	8
	4	256-QAM 5/6	n/a	n/a	720	800	1560	1733.3	3120	3466.7	9
	5	BPSK 1/2					146.3	162.5	292.5	325	0
	5	QPSK 1/2					292.5	325	585	650	1
	5	QPSK 3/4					438.8	487.5	877.5	975	2
	5	16-QAM 1/2					585	650	1170	1300	3
	5	16-QAM 3/4					877.5	975	1755	1950	4
	5	64-QAM 2/3					1170	1300	2340	2600	5
	5	64-QAM 3/4					1316.3	1462.5	2632.5	2925	6
	5	64-QAM 5/6					1462.5	1625	2925	3250	7
	5	256-QAM 3/4					1755	1950	3510	3900	8
	5	256-QAM 5/6					1950	2166.7	3900	4333.3	9
	6	BPSK 1/2					175.5	195	351	390	0
	6	QPSK 1/2					351	390	702	780	1
	6	QPSK 3/4					526.5	585	1053	1170	2
	6	16-QAM 1/2					702	780	1404	1560	3
	6	16-QAM 3/4					1053	1170	2106	2340	4
	6	64-QAM 2/3					1404	1560	2808	3120	5
	6	64-QAM 3/4					1579.5	1755	3159	3510	6
	6	64-QAM 5/6					1755	1950	3510	3900	7
	6	256-QAM 3/4					2106	2340	4212	4680	8

802.11n											802.11ac
HT MCS Index	Spatial Streams	Modulation & Coding	Data Rate GI = 800ns 20MHz	Data Rate SGI = 400ns 20MHz	Data Rate GI = 800ns 40MHz	Data Rate SGI = 400ns 40MHz	Data Rate GI = 800ns 80MHz	Data Rate SGI = 400ns 80MHz	Data Rate GI = 800ns 160MHz	Data Rate SGI = 400ns 160MHz	VHT MCS Index
	7	BPSK 1/2					204.8	227.5	409.5	455	0
	7	QPSK 1/2					409.5	455	819	910	1
	7	QPSK 3/4					614.3	682.5	1228.5	1365	2
	7	16-QAM 1/2					819	910	1638	1820	3
	7	16-QAM 3/4					1228.5	1365	2457	2730	4
	7	64-QAM 2/3					1638	1820	3276	3640	5
	7	64-QAM 3/4					n/a	n/a	3685.5	4095	6
	7	64-QAM 5/6					2047.5	2275	4095	4550	7
	7	256-QAM 3/4					2457	2730	4914	5460	8
	7	256-QAM 5/6					2730	3033.3	5460	6066.7	9
	8	BPSK 1/2					234	260	468	520	0
	8	QPSK 1/2					468	520	936	1040	1
	8	QPSK 3/4					702	780	1404	1560	2
	8	16-QAM 1/2					936	1040	1872	2080	3
	8	16-QAM 3/4					1404	1560	2808	3120	4
	8	64-QAM 2/3					1872	2080	3744	4160	5
	8	64-QAM 3/4					2106	2340	4212	4680	6
	8	64-QAM 5/6					2340	2600	4680	5200	7
	8	256-QAM 3/4					2808	3120	5616	6240	8
	8	256-QAM 5/6					3120	3466.7	6240	6933.3	9

Parts de marché



Taille et prévisions des parts de marché mondial et régional trimestrielles des équipements WLAN et téléphones WiFi : Quatrième trimestre 2014

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

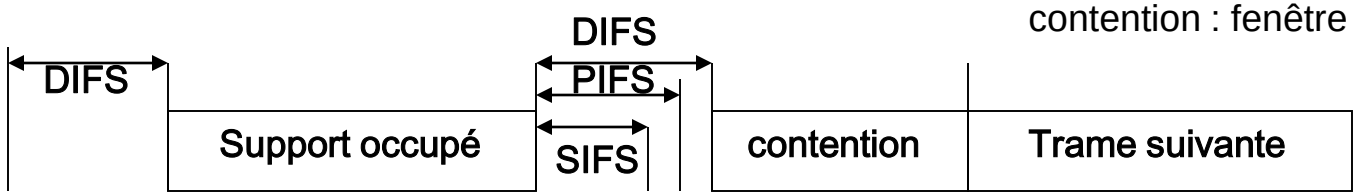
Méthode d'accès

- **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**

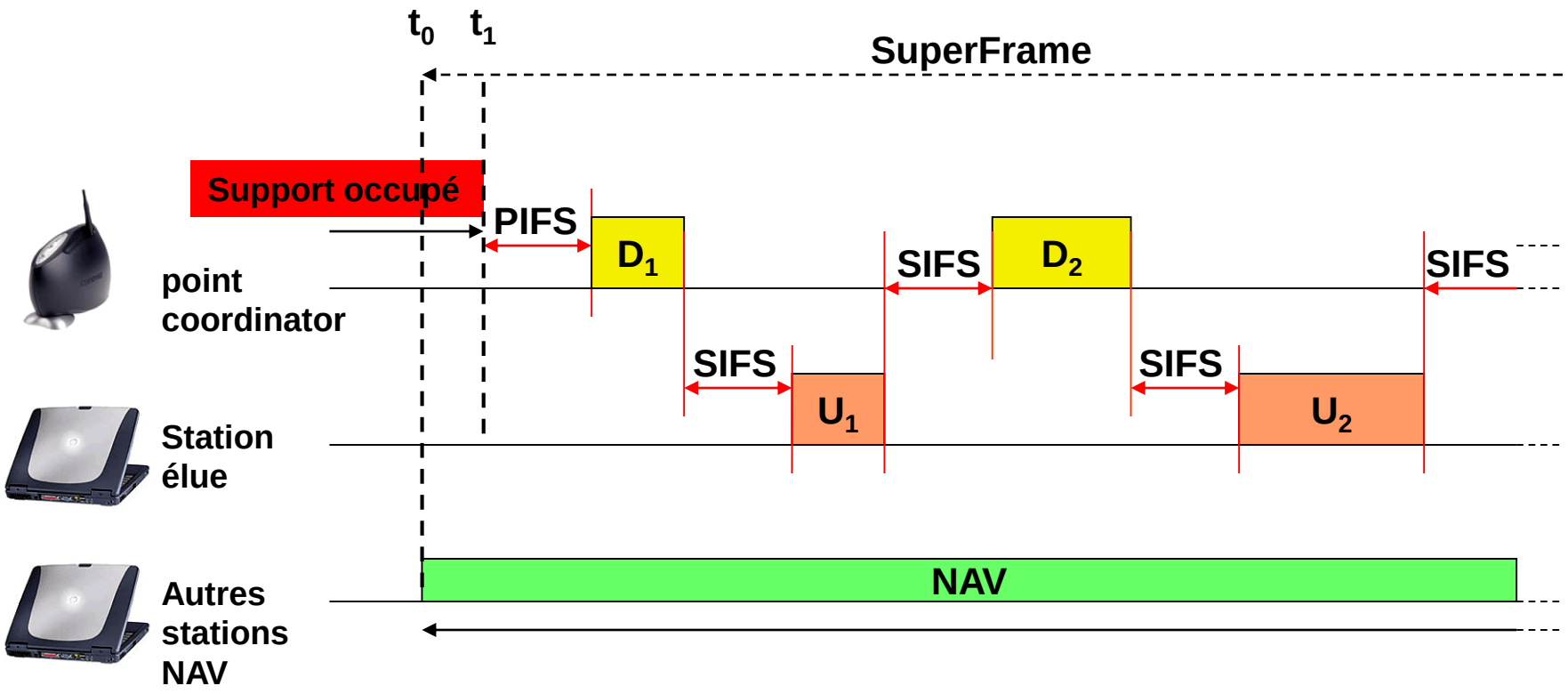
Méthode d'accès

CSMA/CA est basé sur :

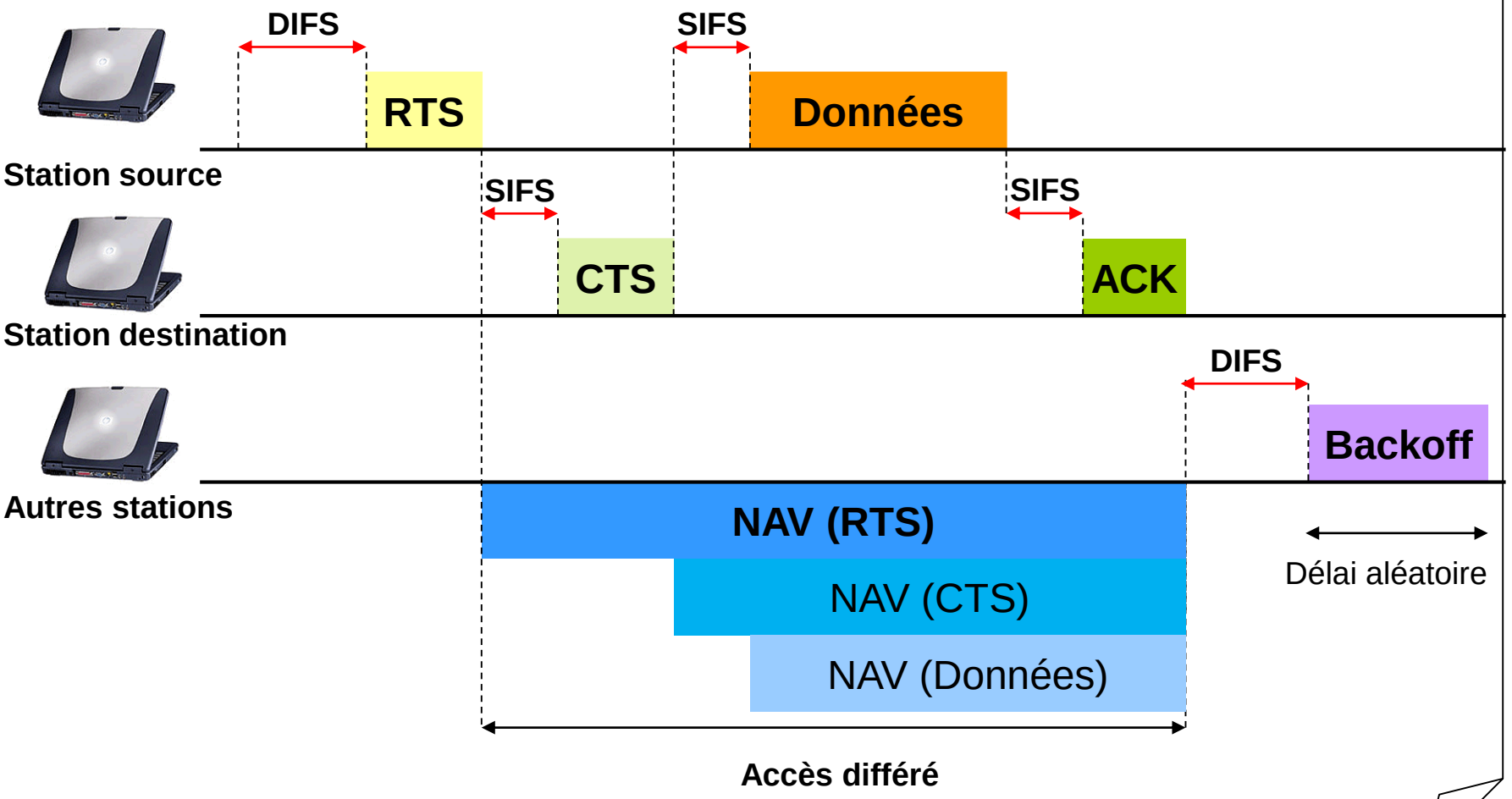
- L'écoute du support :
  - Mécanisme de réservation du support (Ready To Send /Clear To Send)
  - Network Allocation Vector (NAV)
- Les temporisateurs IFS (Inter Frame Spacing)
  - SIFS (Short IFS) : Plus haute priorité pour ACK, CTS interrogations en PCF
  - PIFS (PCF IFS) : Priorité Moyenne, pour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



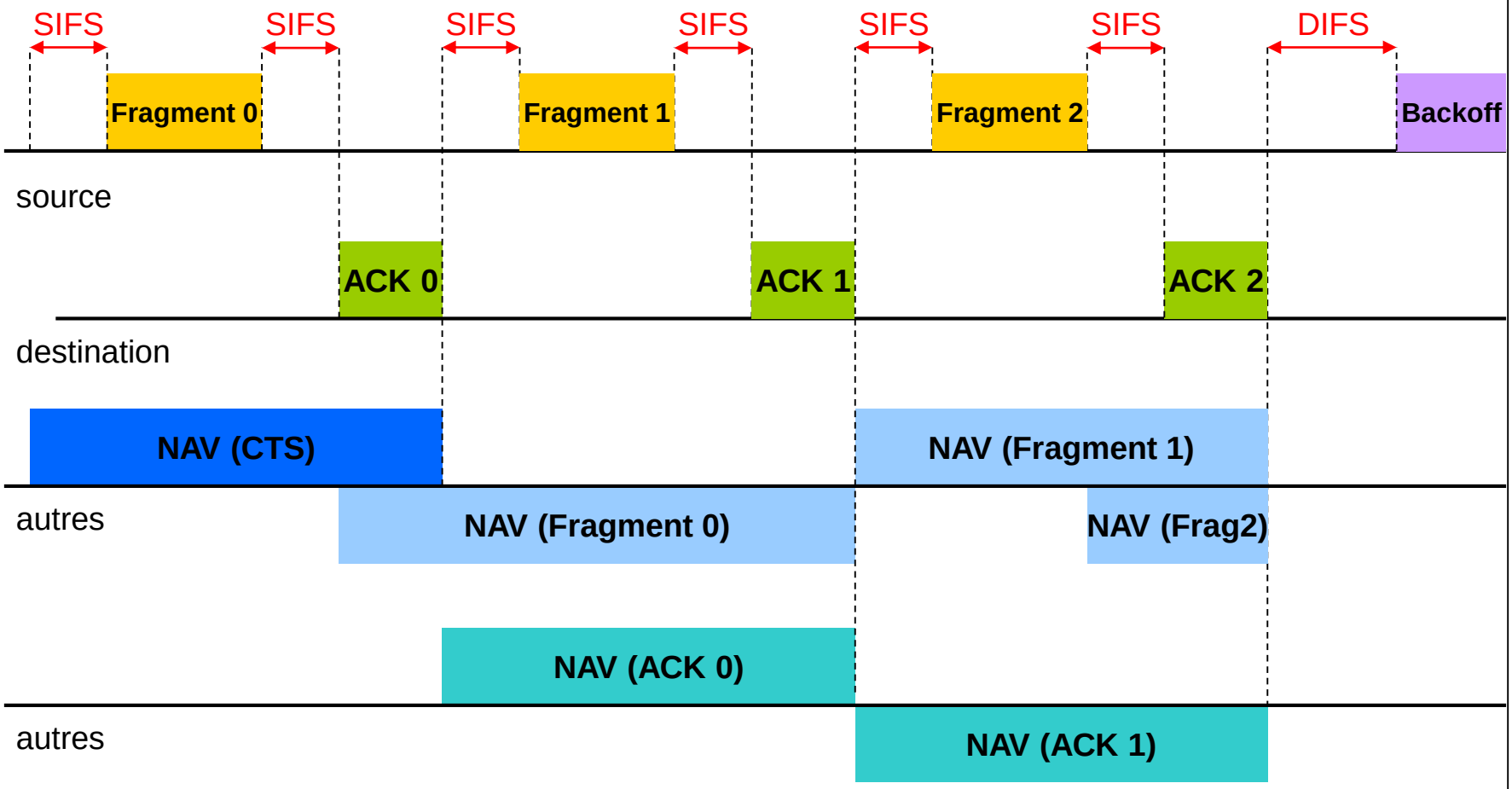
PCF (Point Coordination Function)

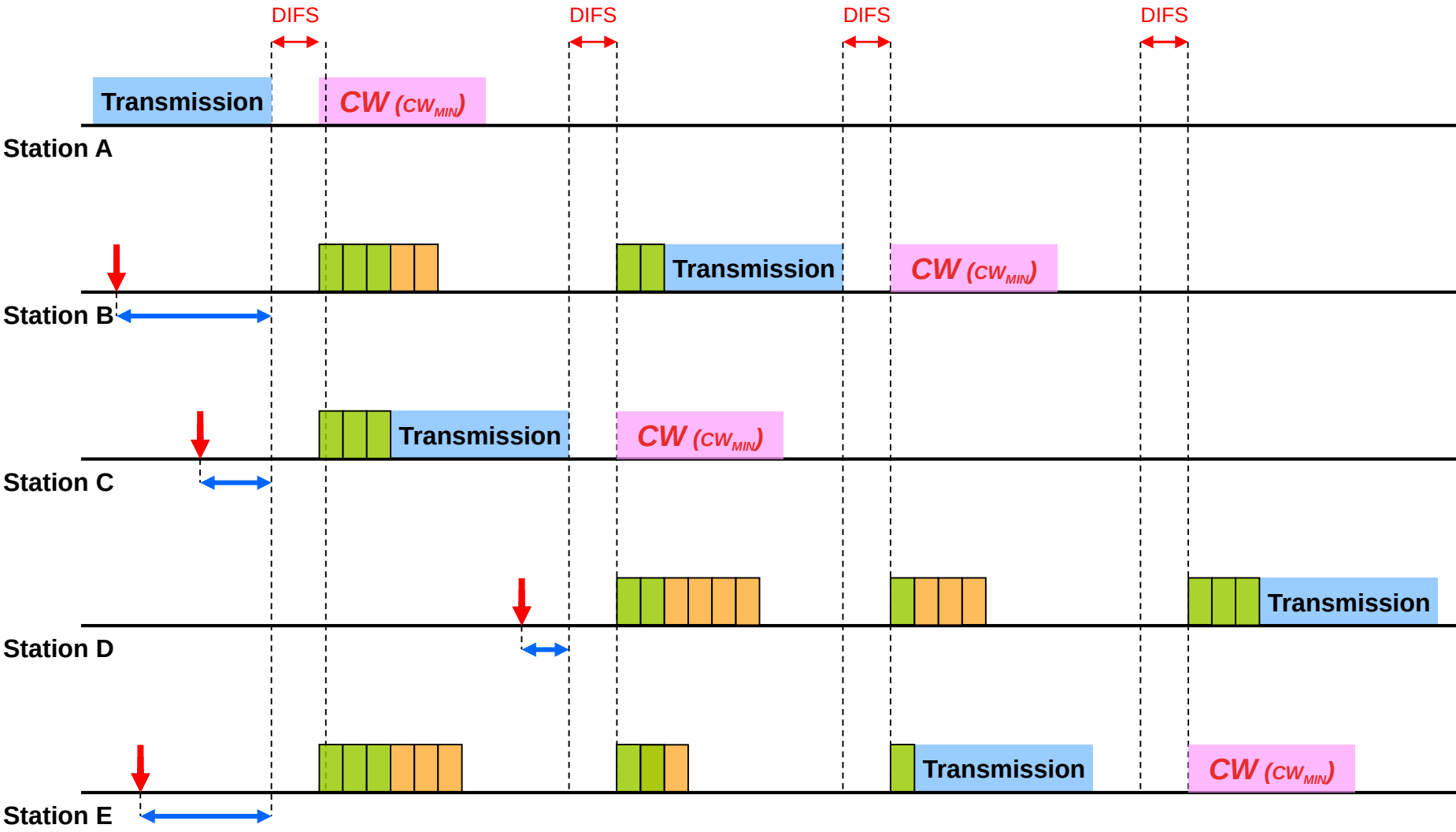


DCF (Distributed Coordination Function)

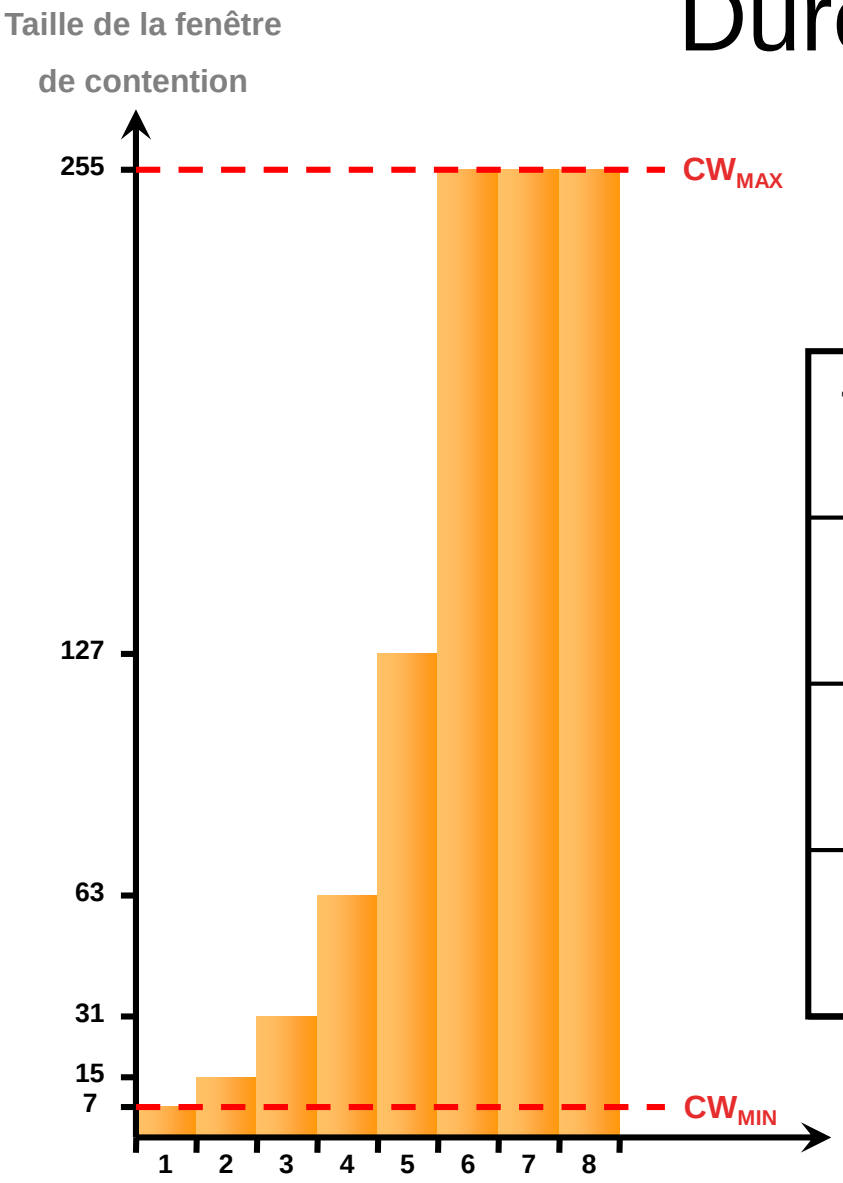


Supports empruntés à G. Pujolle


SIFS
SIFS
SIFS
SIFS
SIFS
SIFS
DIFS
Fragment 0
Fragment 1
Fragment 2
Backoff
source
ACK 0
ACK 1
ACK 2
destination
NAV (CTS)
NAV (Fragment 1)
autres
NAV (Fragment 0)
NAV (Frag2)
NAV (ACK 0)
autres
NAV (ACK 1)


DIFS
DIFS
DIFS
DIFS
Transmission
CW (CWMIN)
Station A
Transmission
CW (CWMIN)
Station B
Transmission
CW (CWMIN)
Station C
Transmission
Station D
Transmission
CW (CWMIN)
Station E
Légende :
Timeslot expiré
Timeslot restant
La station accède et écoute le support
Temps d'attente dû à l'occupation du support par une autre station
CW (CWMIN)
Taille de la fenêtre de contention

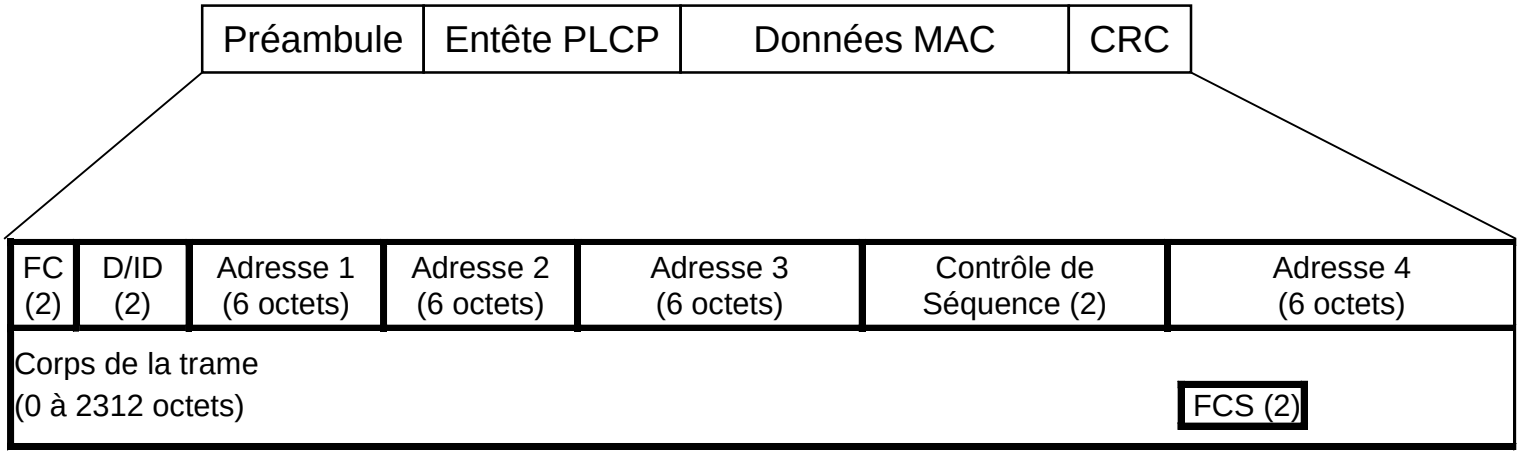
Durées



	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

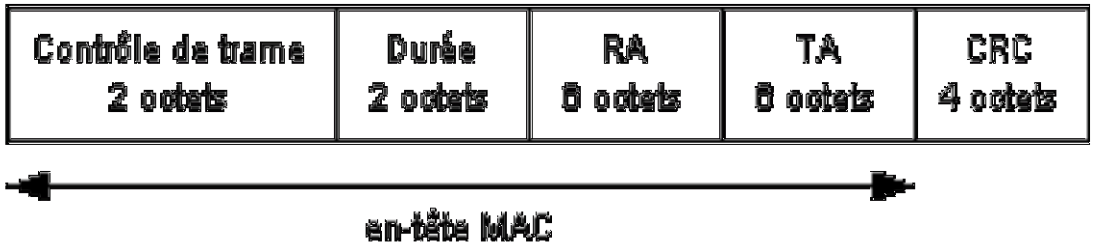
FC (2)	D/ID (2)	Adresse 1 (6 octets)	Adresse 2 (6 octets)	Adresse 3 (6 octets)	Contrôle de Séquence (2)	Adresse 4 (6 octets)
Corps de la trame (0 à 2312 octets)						FCS (2)

Version de protocole (2 bits)		Type (2 bits)		Sous-Type (4 bits)			
To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)

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

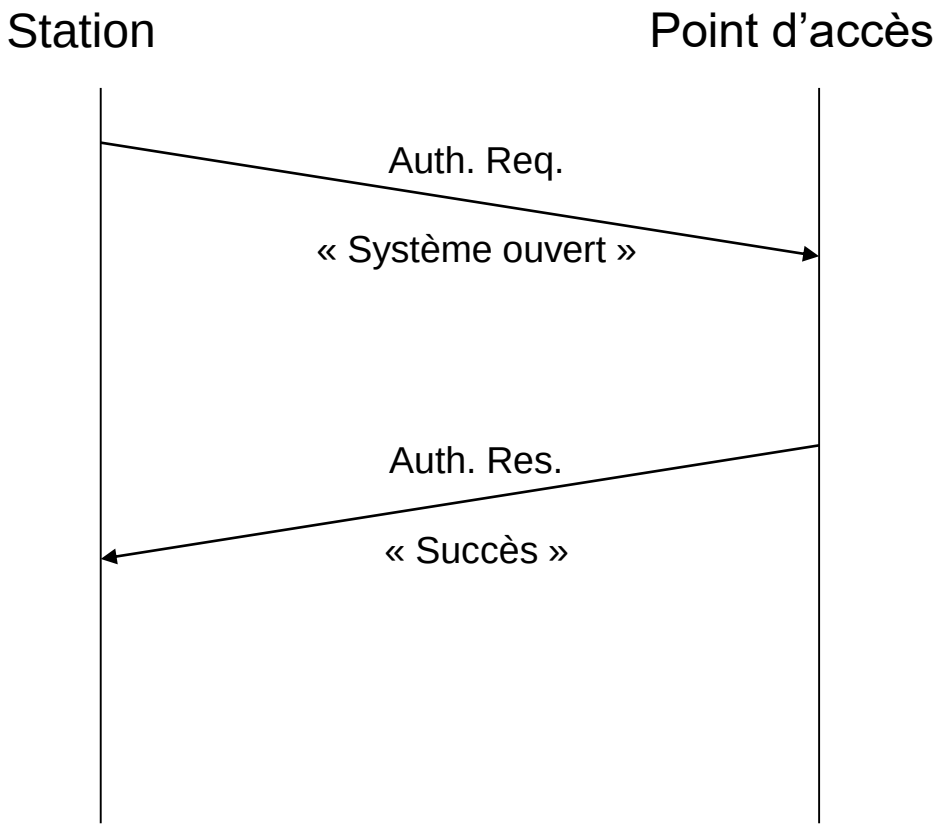
Sécurité

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

Authentification

- Dans un système ouvert



Quelques solutions…

- Ecoute clandestine :
  - Chiffrement des données
- Intrusion ou usurpation
  - Limiter l'accès radio et l'accès réseau
  - Authentifier les personnes
  - Désactiver le serveur DHCP (perte de souplesse pour peu de sécurité)

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, bluetooth, micro-ondes…

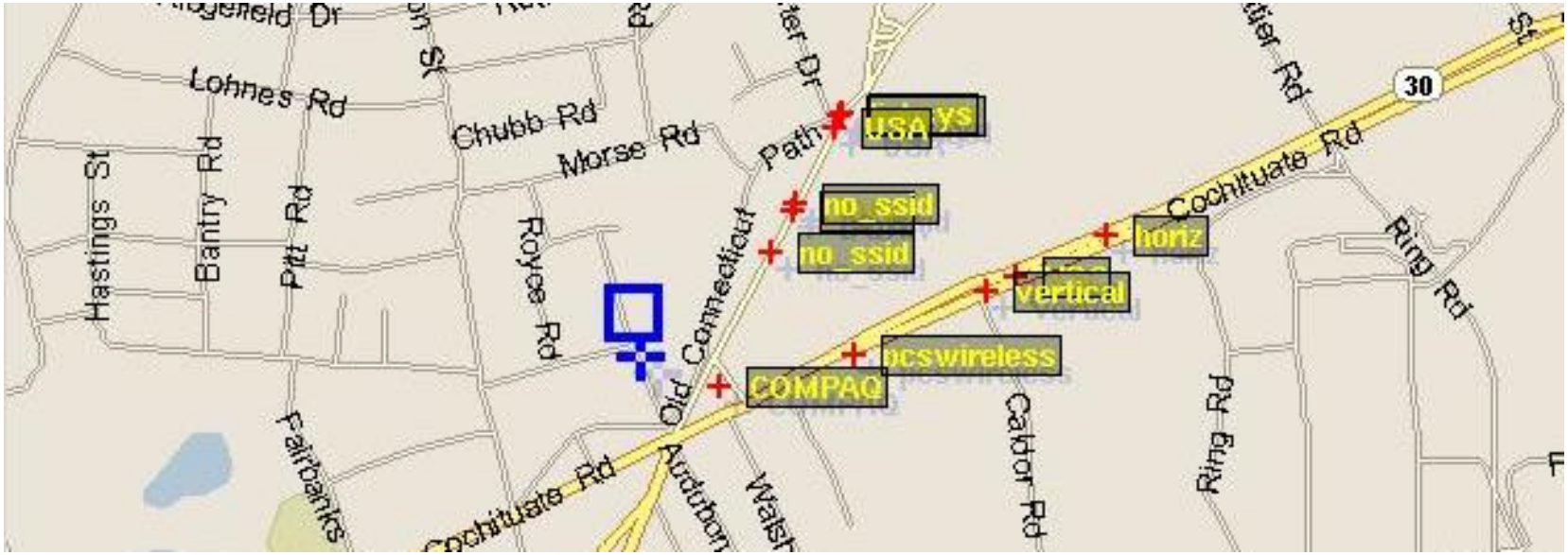
Les attaques : refus de service

- **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

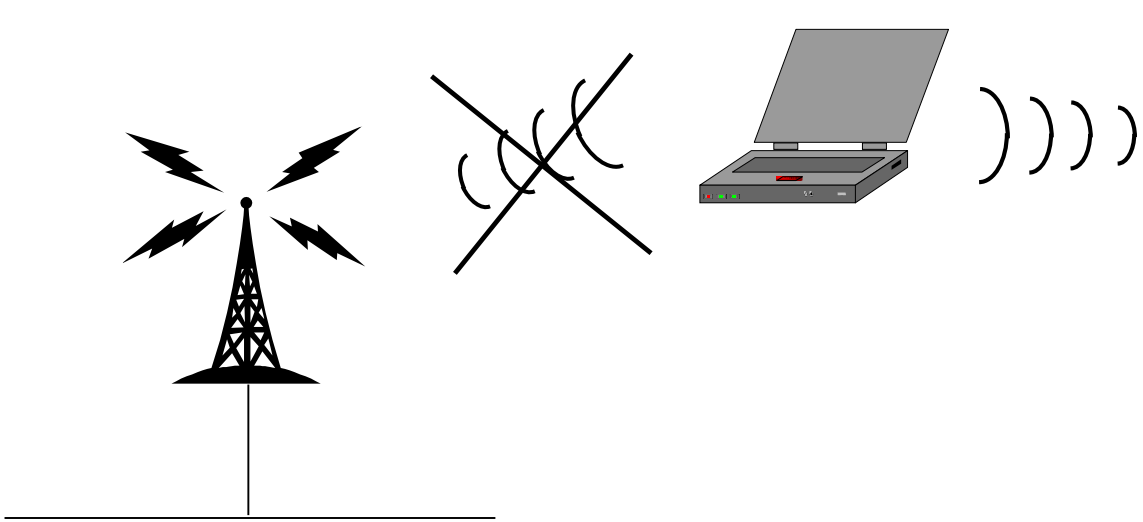
Un jeu : le **War Driving** = Quadrillage d'une ville avec

- ✓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

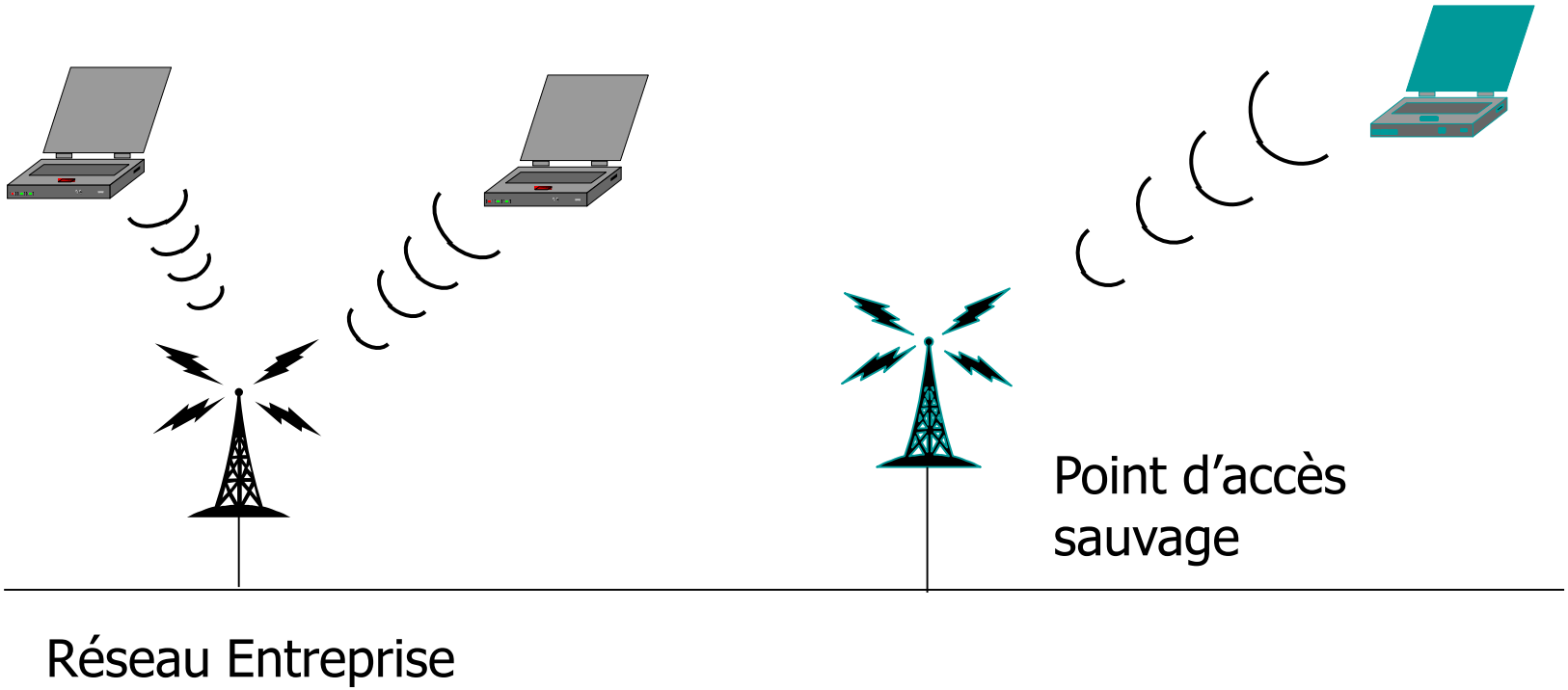
- Point d'accès «malicieux»



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

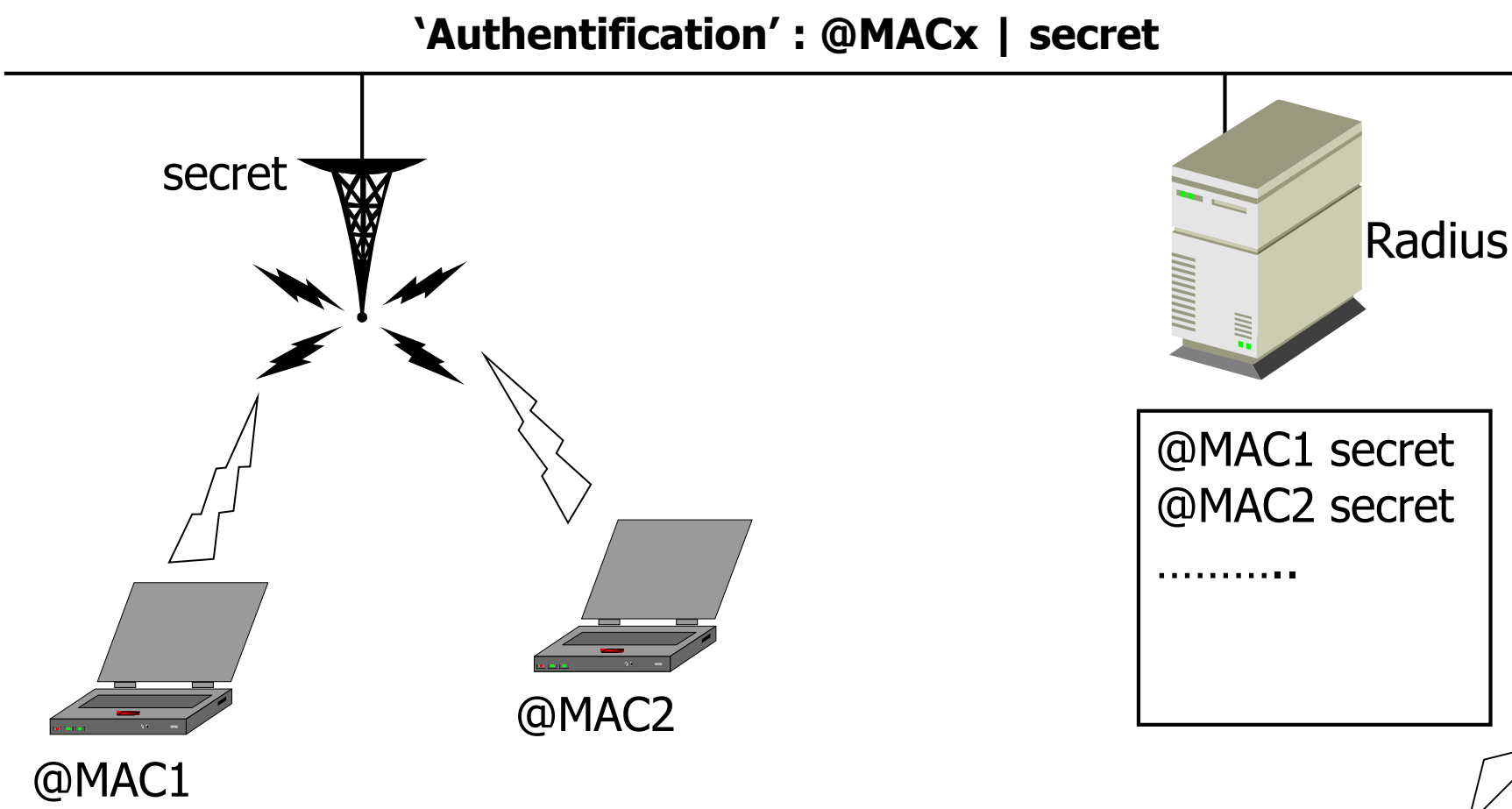
- N’autoriser que certaines adresses à se connecter aux points d’accès.

- 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"

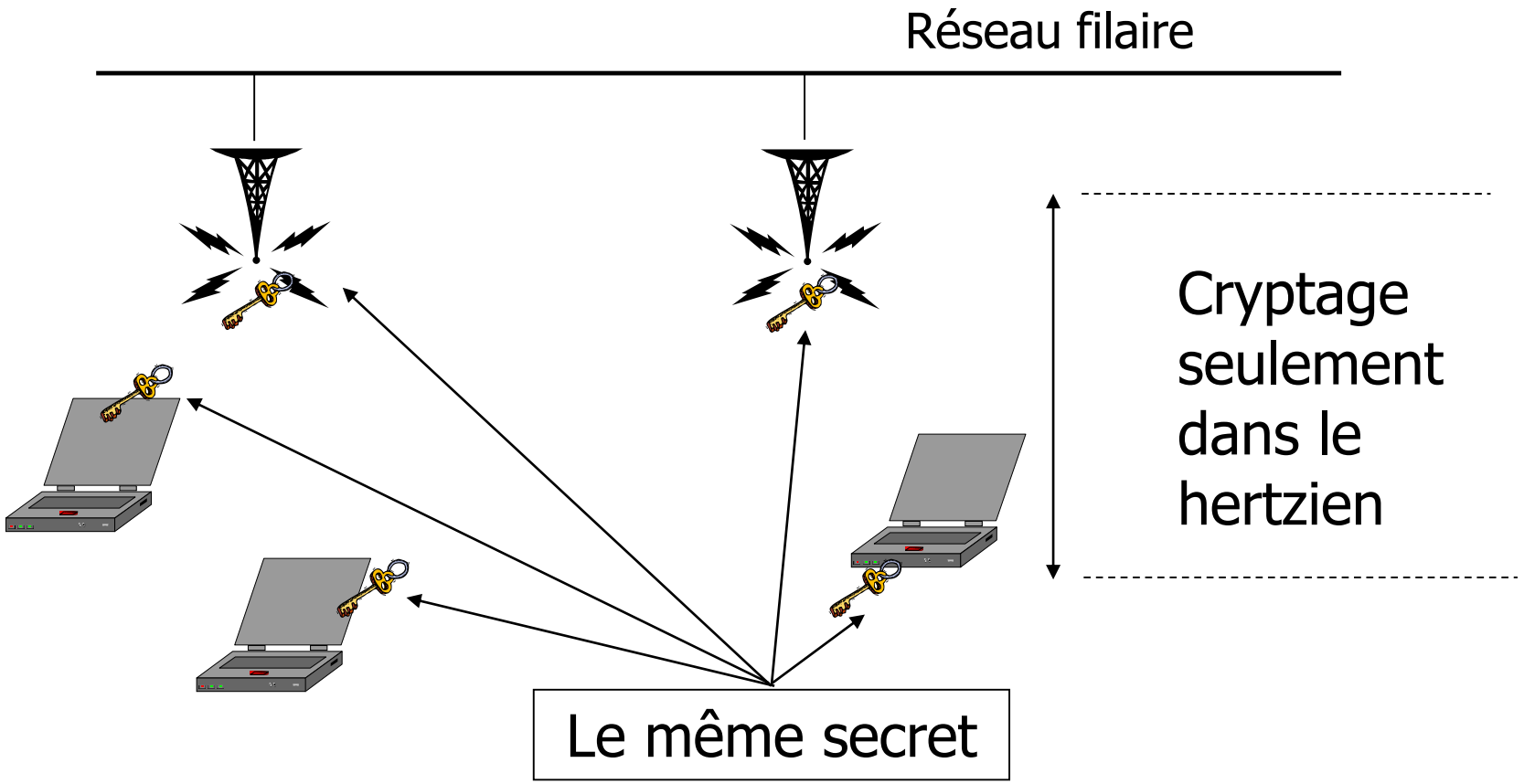
Wired Equivalent Privacy

- Objectif :
  Offrir une solution de chiffrement 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.

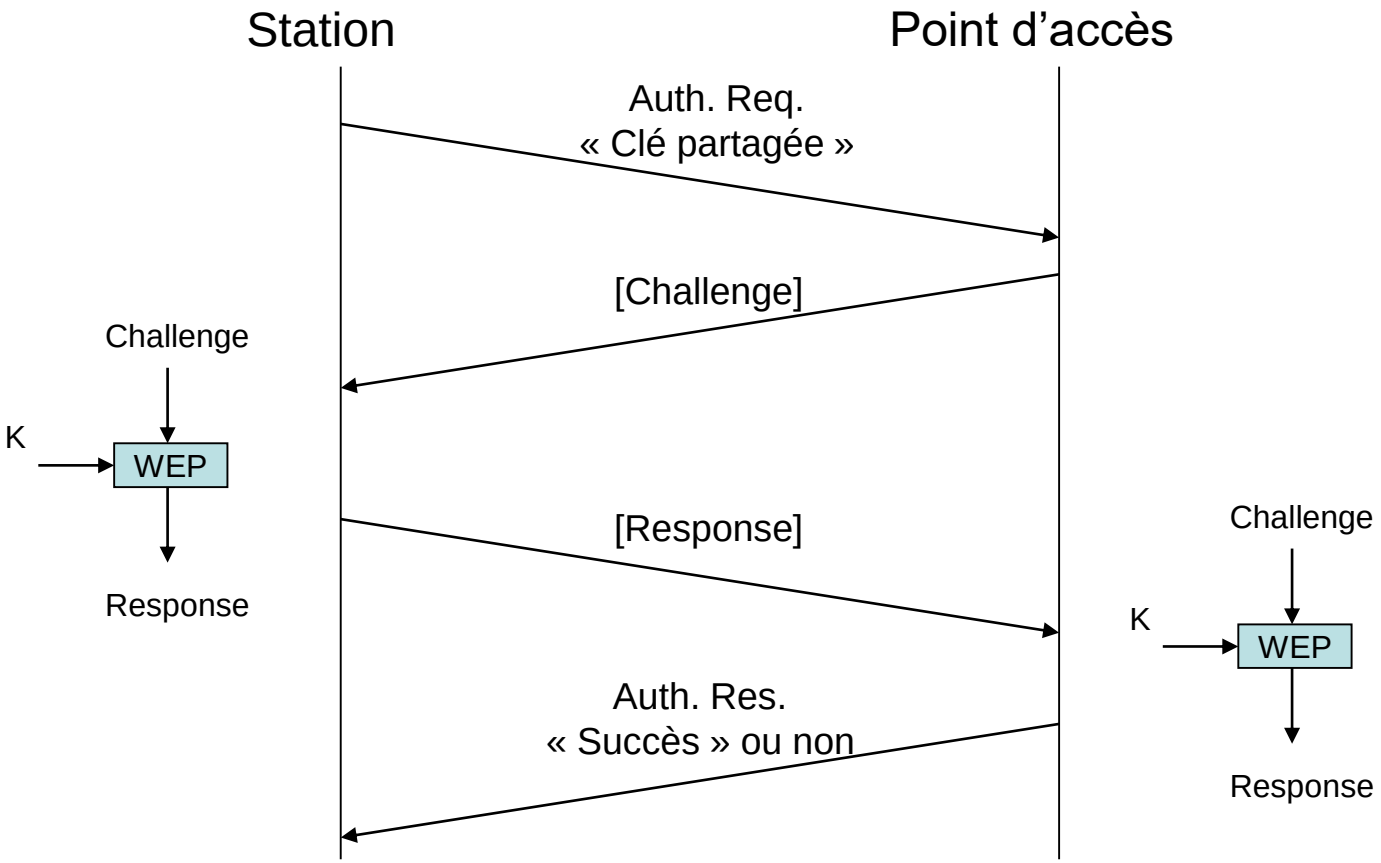
  Le chiffrement n'est utilisé qu'entre les éléments 802.11. Il ne s'applique plus sur le réseau filaire.

Wired Equivalent Privacy



Authentification

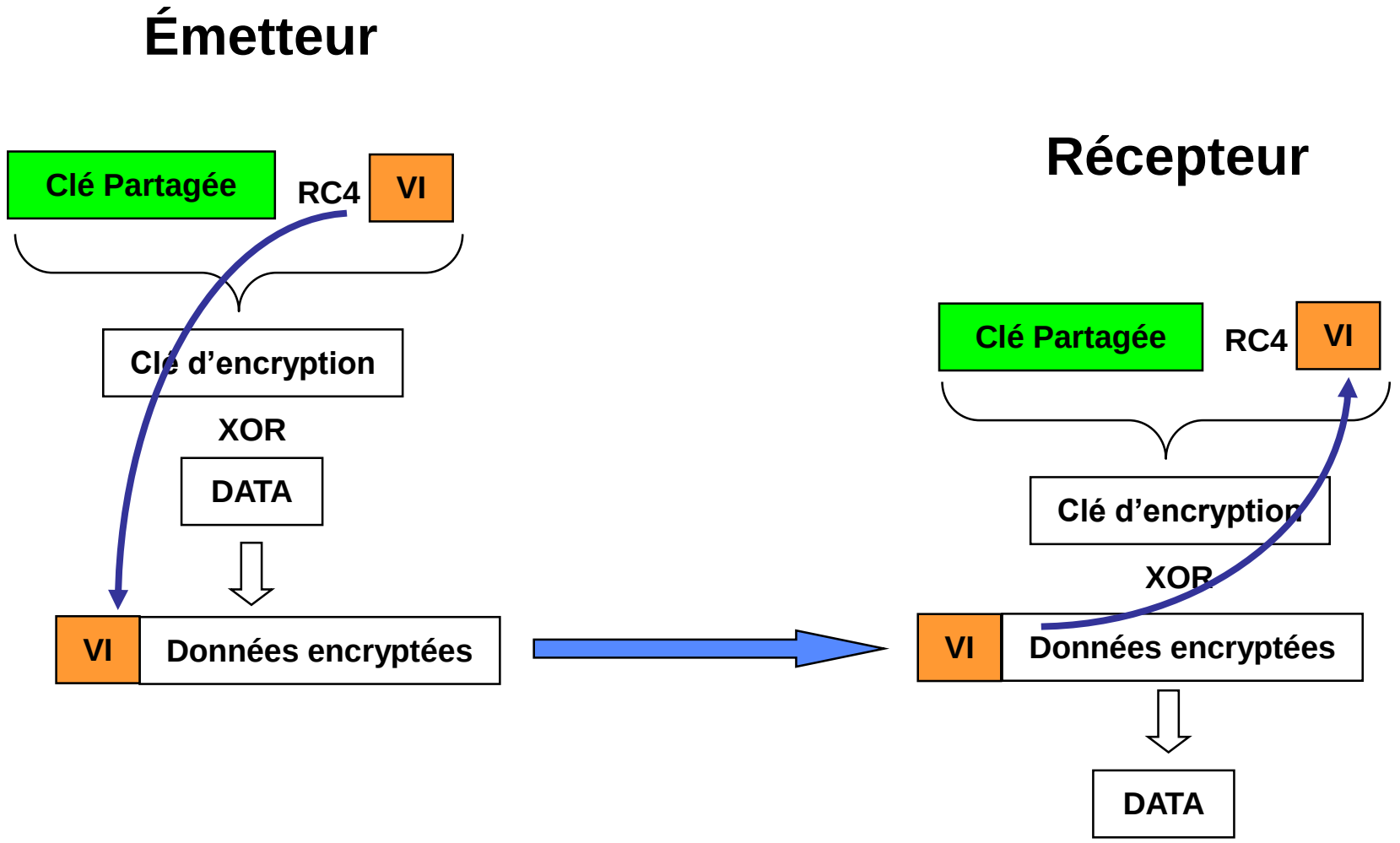
- Dans un système à clé partagée (WEP)



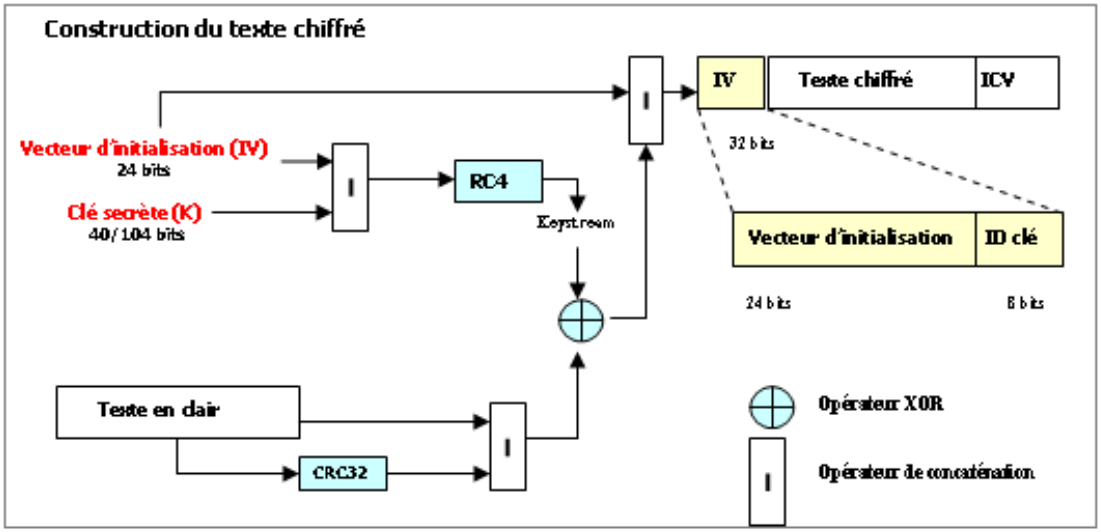
WEP – les points faibles

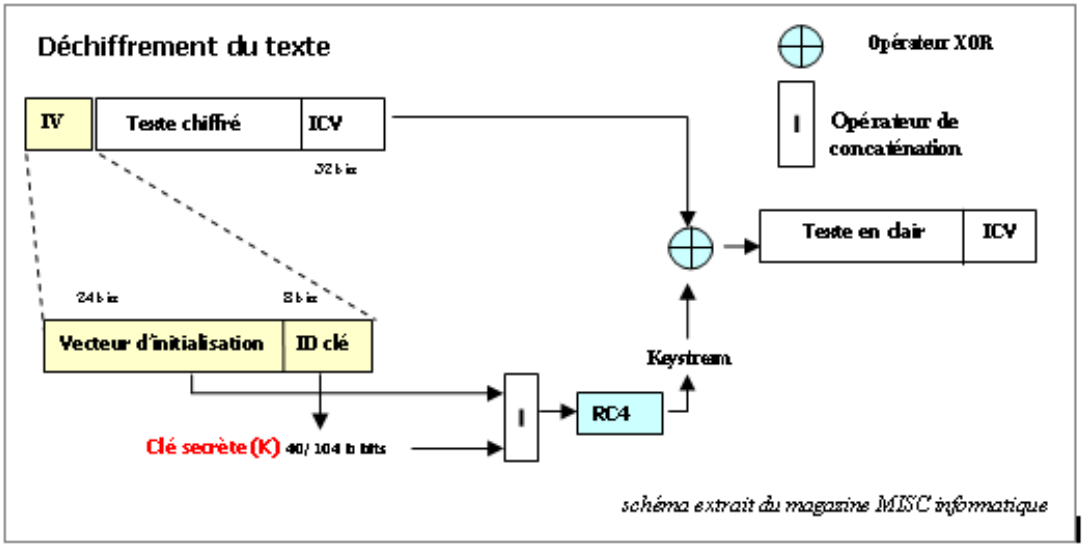
- Clés statiques partagées (40 bits "64", 104 bits "128")
  - Rarement changées
  - Vol de machine => vol de clef
  - Les autres qui partagent la clef peuvent lire vos trames
  - Possède une durée de vie longue
  - Diffusion d'une nouvelle clé difficile si le parc de mobile est important.
- Possibilité 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

- WPA : authentification + chiffrement
  - Respecte la norme 802.11i
  - Chiffrement TKIP
    (Temporal Key Integrity Protocol)
  - Authentification :
    - Personnel : WPA – PSK
    - Entreprise : 802.1x – EAP avec serveur Radius

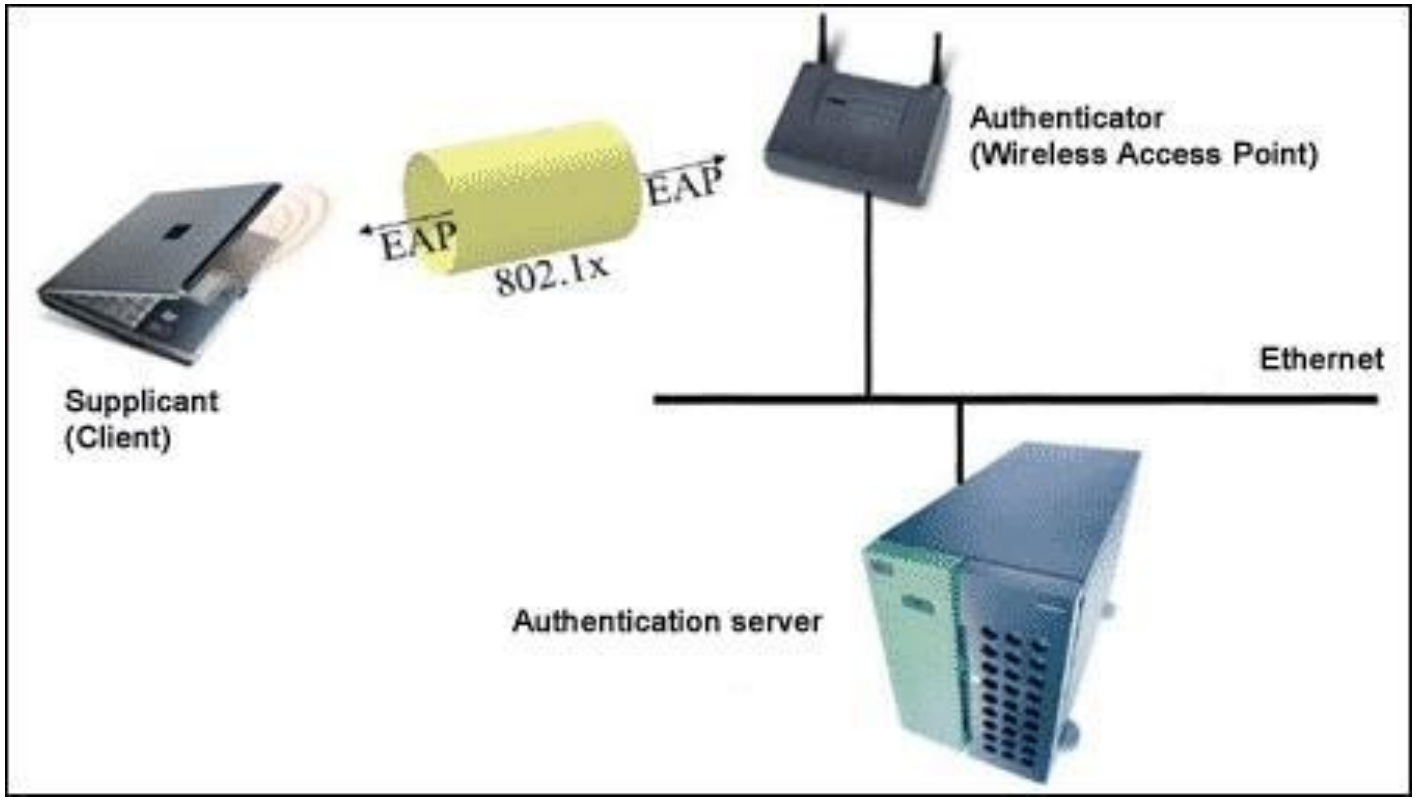
La sécurité avec le 802.1x

- 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

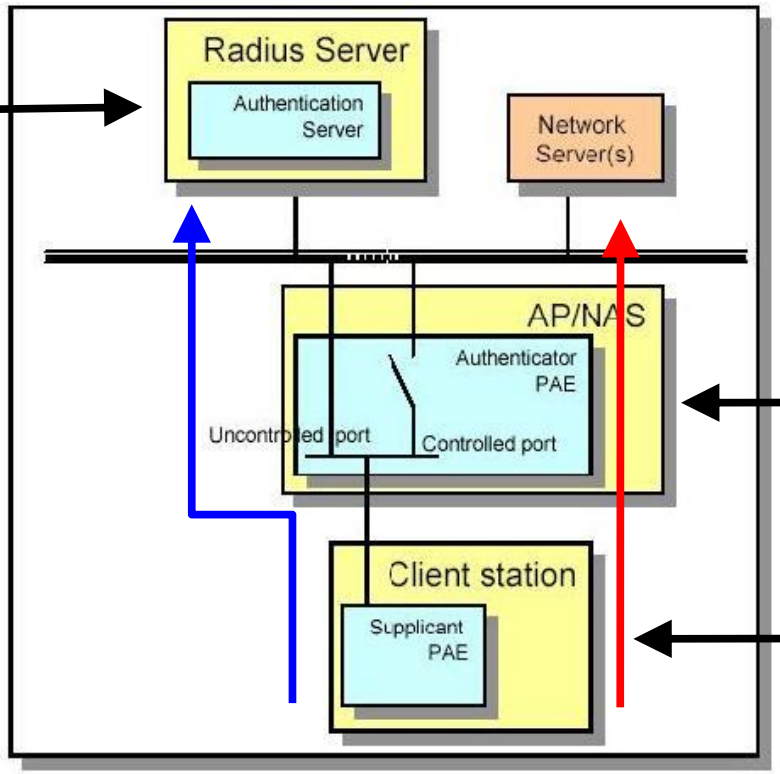


Les trois différents rôles dans le IEEE 802.1X: Supplicant, Authenticator et Authentication Server (AAA Server: EAP Server, généralement RADIUS).

802.1x: Le Dual-port

- Principe

Serveur d'Authentification (Contrôle des mots de passe ou certificats)



Point d'accès sans fil

Ordinateur portable + carte Wifi

PAE : Port Access Entity
NAS : Network Access Server
AP : Access Point

Trafic authentifié
Trafic non-authentifié

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
- une solution finale incompatible avec le matériel existant où 802.1X est obligatoire, avec l'algorithme de chiffrement RC4 remplacé par AES.

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.**

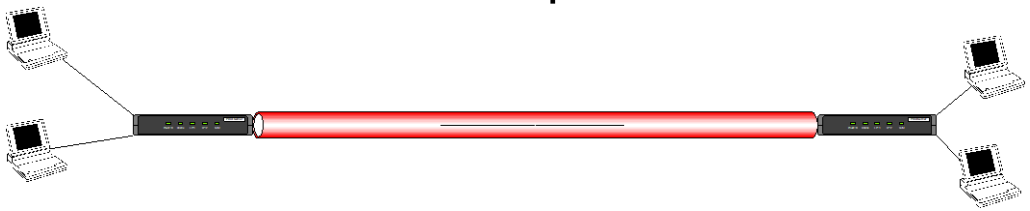
VPN : Les réseaux privés virtuels

- **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 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)

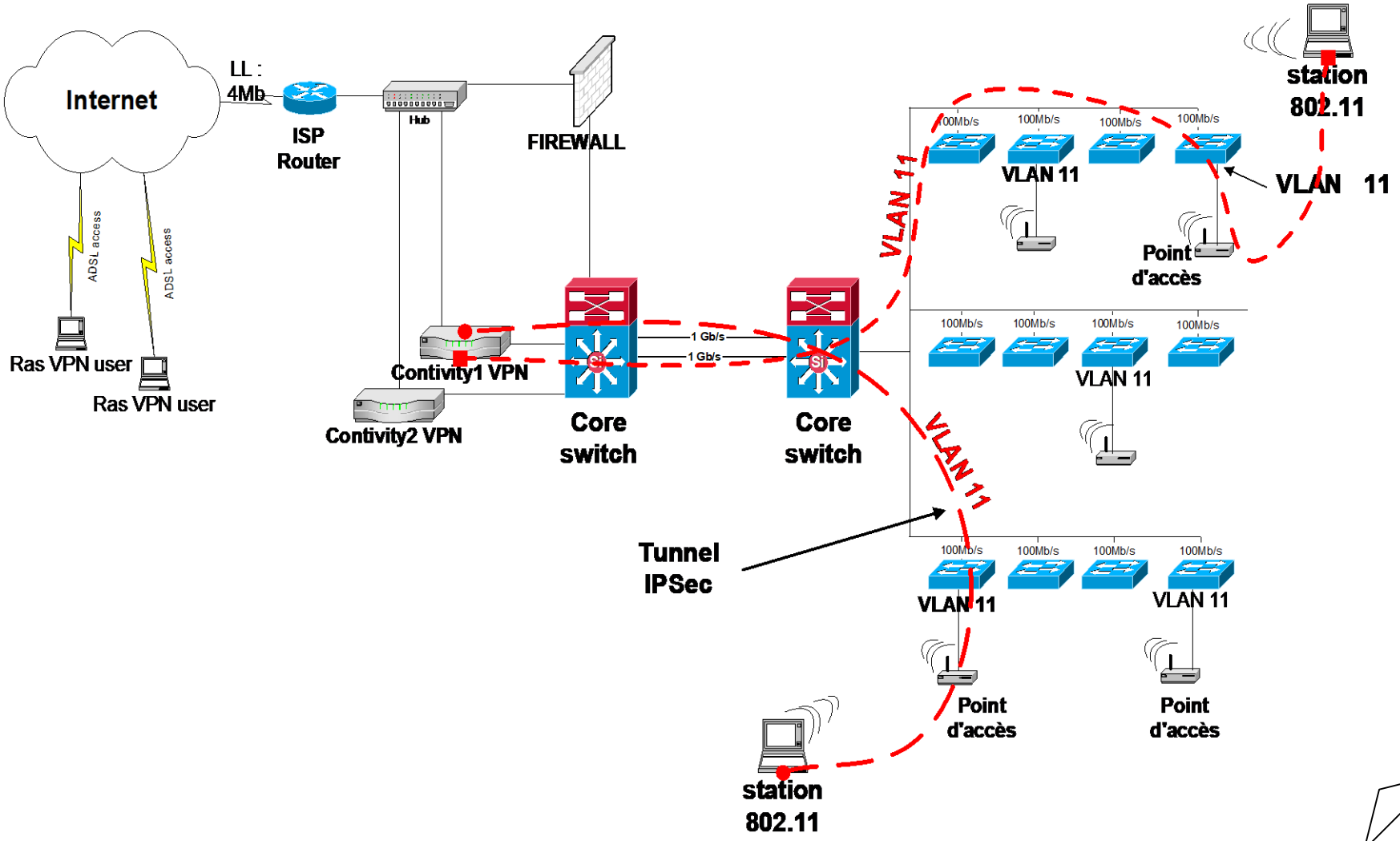
IPSec appliqué aux VPN

- **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.

- 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.

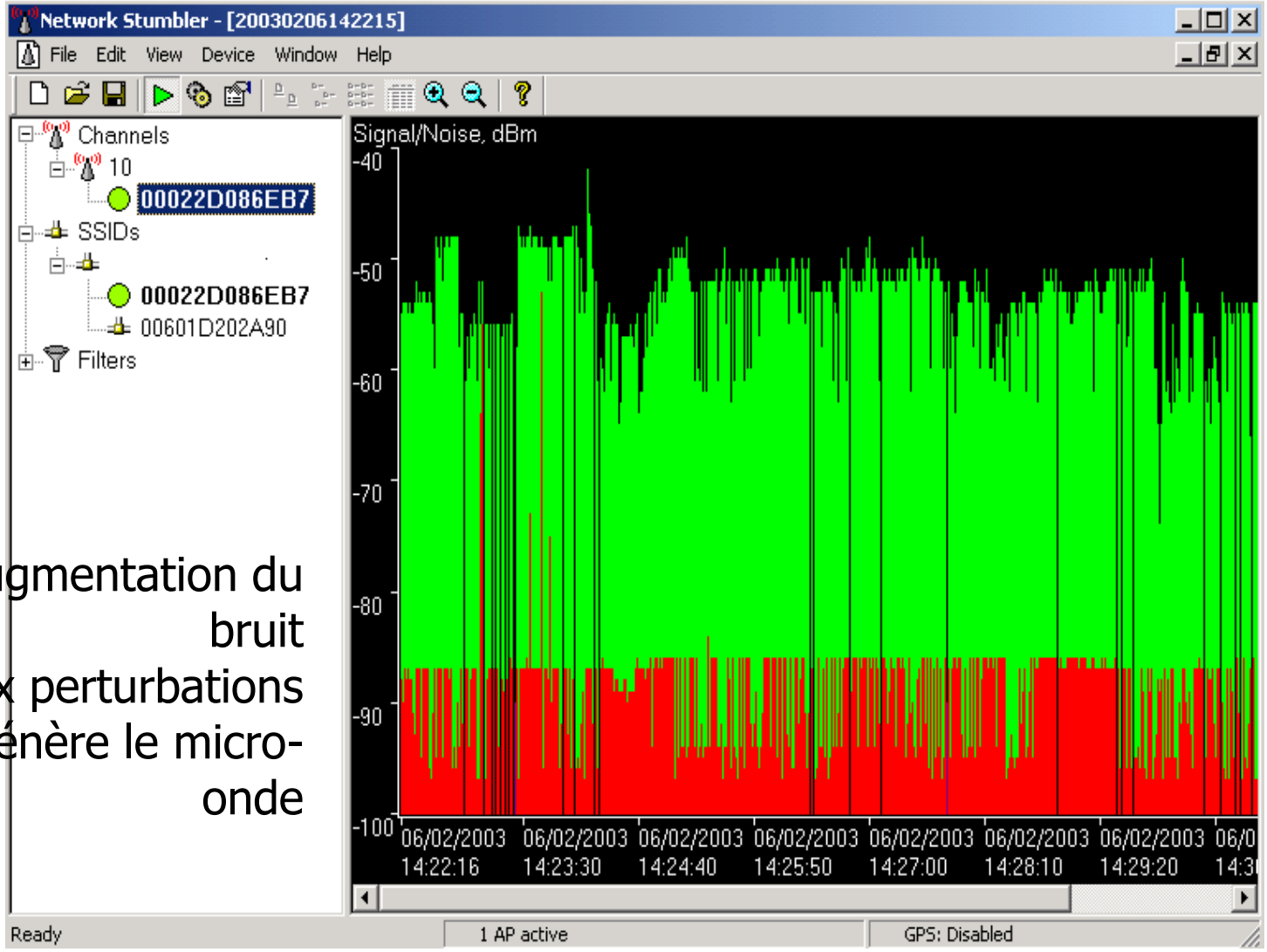
Architecturer correctement ses WLAN

- 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

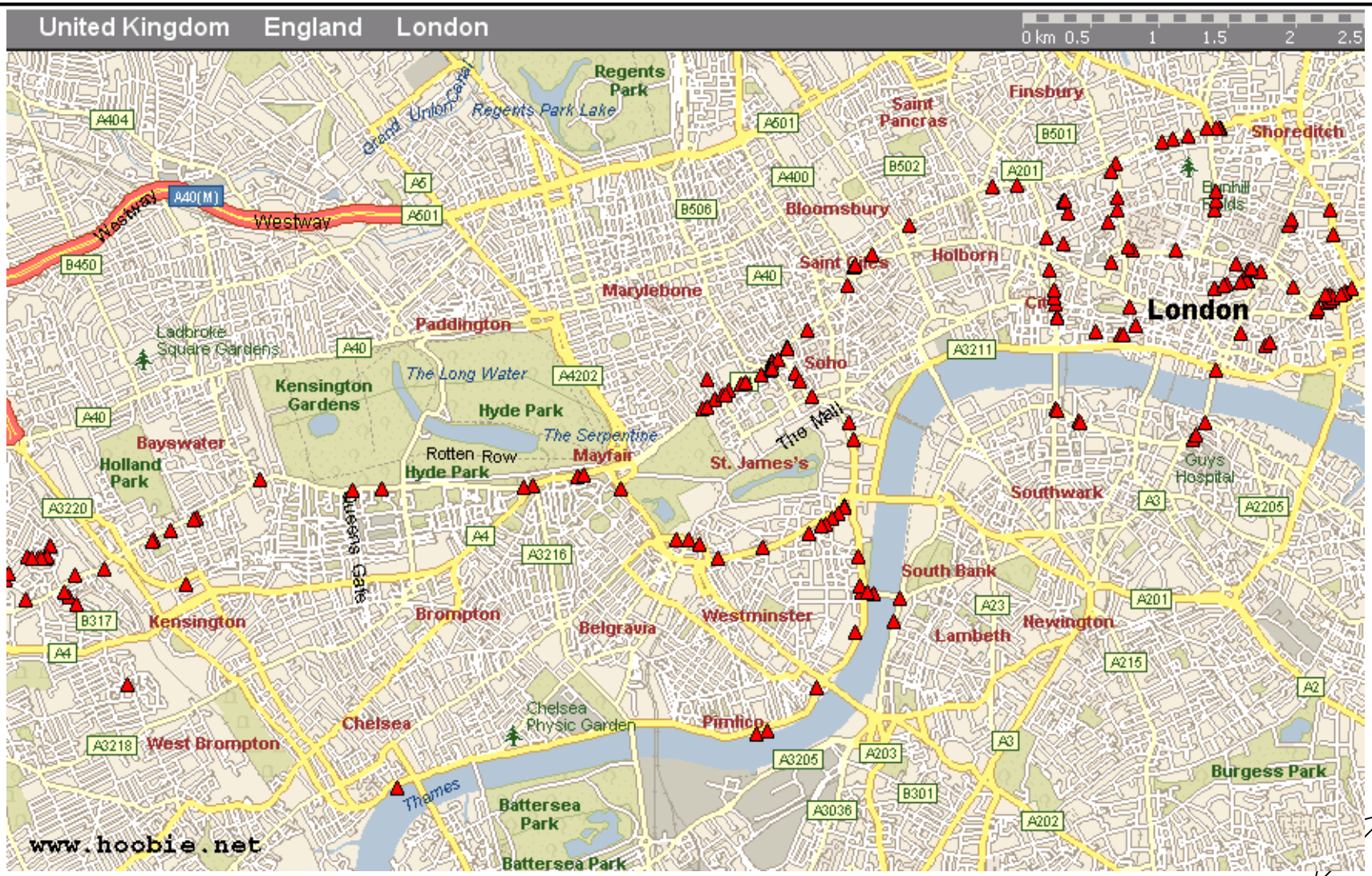
- Netstumbler (http://www.netstumbler.com)
  - Fournit peu d'information.
  - Interface conviviale.
  - Historique ratio signal/bruit.
  - Fonctionne avec différentes cartes (Cisco, Orinoco, Netgear, …).
- Netstumbler pour Ipaq
  - Plus petit et plus discret

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 existent.

- **Ou WPA2.**

- **Ou utiliser VPN avec IPSec**.
  Si le parc est hétérogène. C'est la solution la plus utilisée lorsque le WLAN est sécurisé.