Technique de base des Réseaux WIFI

26-27 Avril 2018

Cabaré Michel

**Table des matières**

réseaux sans fils 4

Présentation: 4

réseaux sans fils et ARCEP 5

ARCEP Autorité de Régulation Communication Electronique et des Postes: 5

Wifi – déclaration ou non: 5

Puissance des canaux - Pire 6

Obligation "légales" 7

Les Liaisons Wi-Fi 8

Structure des liaisons: 8

Fonctionnement "AD-HOC" (IBSS): 8

Fonctionnement "Infrastructure": 9

Comment une station rejoint-elle une cellule existante ? 10

Le processus d’authentification 11

Le processus d’association - réassociation 11

Le roaming- handover 11

Sécurité 12

L’économie d’énergie 12

Normes Ethernet 802.11 … 13

Panels des Normes 802.11 13

Les anciens 802.11a – 802.11b et 802.11g : 13

802.11b en 1999 – label WI-FI 13

802.11a en 1999 13

802.11g en 2003 14

Bande 2.4 Ghz - gestion des 13 canaux 802.11b-g partage de charge 14

Les nouveaux 802.11n – 802.11ac: 16

Bande 5 Ghz - gestion des 19 canaux 802.11n-ac 17

Sécurité et Wi-Fi 18

WEP Wired Equivalent Privacy - 802.11a - b/g 18

Evolution WPA – WPA2 (TKIP CCMP-AES) 802.11i 18

WPA : Wireless Protection Access 18

WPA 2 - 802.11i 18

RADIUS Remote Authentification Dial In User Service 19

Mémo en 10 points : 19

Lexique WI-FI 20

AES : 20

Adresse MAC : 20

Ad-Hoc : 20

Acces Point - Ap: 20

BSS - Basic Service Set -: 20

DHCP : 20

EAP: 20

Egal à egal: 21

ESS - Extended Service Set: 21

ESSID ou nom du réseau WIFI : 21

IBSS - Independant Basic Service Set: 21

MIMO - Multiple-Input Multiple-Output: 21

Mode Infrastructure: 21

Pire : 21

PSK : 21

Point d’Accès : 22

Radius Remote Authentification Dial-In User Service 22

Roaming 22

SSID ou ESSID ou nom du réseau WIFI : 22

WEP 22

Wi-Fi 22

WPA 22

WPA 2 22

ANNEXE 23

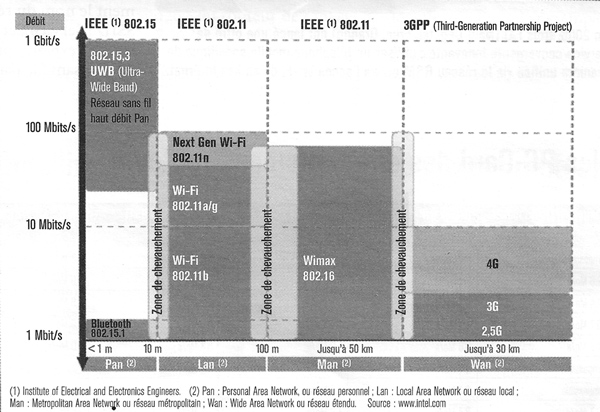
cas pratique de gestion des canaux : 23

# réseaux sans fils

## Présentation:

Dans les technologies mobiles ont peut discerner :

* Les **WPAN** (**Wireless Personal Area Network**) : avec des marques telles que Bluetooth, HomeRF
* Les **WLAN** (**Wireless Local Area Networks**) : avec deux standards principaux, IEEE 802.11 (US) sur des ondes radio 2.4 Ghz ou 5Ghz avec un débit symétrique de 50Mbit/s sur 100m et Hiperlan (Europe)
* Le **WMAN** (**Wireless Metropolitan Area Networks**) ou **Wimax** qui est une sorte de WIFI longue portée basée sur des ondes radio 3.5Ghz avec un débit symétrique de 75Mbit/s sur 50km
* Les technologies cellulaires (**GSM**, **GPRS**, **UMTS**)



Dans le spectre de la WIFI, 2 technologies principales:

* Une **WPAN** (**Wireless Personal Area Network**) : avec la norme **Bluetooth** lancée à l’origine en 1994 par Ericsson qui touche le domaine de la domotique. Après une première spécification en 1999 puis une deuxième en 2004, travaille à 2.4 GHz soit la même bande que le WI-FI

1Mb/s Full Duplex,puis 10Mb/S en 2004, portée de 10 m (1 mW)

* Une **WLAN** (**Wireless Local Area Networks**) : avec le standard principal, **802.11** ou **WIFI** de l’IEEE sera traité dans un chapitre spécifique.

Ces 2 protocoles ne sont absolument pas compatibles entre eux.

# réseaux sans fils et ARCEP

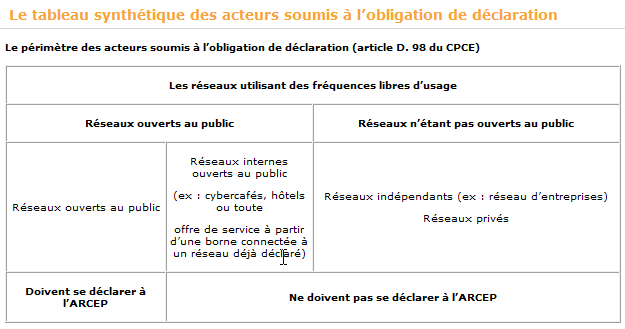
## ARCEP Autorité de Régulation Communication Electronique et des Postes:

**http://www.arcep.fr**

…la bande 5 GHz est également ouverte aux systèmes Wi-Fi dans un cadre spécifique. La décision n° 2008-0568 de l'ARCEP autorise ainsi les systèmes Wi-Fi à fonctionner dans les fréquences 5250-5350 MHz et 5470-5725 MHz, en imposant la mise en œuvre d'un mécanisme de sélection dynamique de fréquences (DFS) et un mécanisme de régulation de la puissance de l'émetteur. Ces modalités sont nécessaires afin de garantir un fonctionnement compatible avec les systèmes radars utilisant ces bandes de fréquences…

## Wifi – déclaration ou non:

Par " opérateur ", on entend toute personne physique ou morale qui exploite un réseau de communications électroniques ouvert au public ou qui fournit au public un service de communications électroniques (art. L.32 du code des poste et des communications électroniques).



* Un réseau est " ouvert au public " dès lors qu’il est établi ou utilisé pour fournir des " services de communication au public par voie électronique " à l’attention du public

L’absence de déclaration Arcep

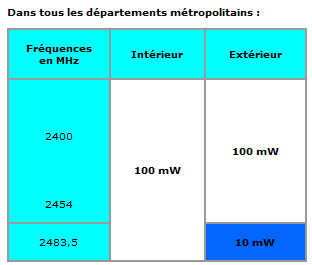
* Un réseau Wi-Fi localisé à un bâtiment ou une zone réduite rentre dans cette qualification de « réseau interne ouvert au public ». Ceci concerne toute structure : cybercafés, bureaux, hôtels, bibliothèque. Ils peuvent implanter et mettre à disposition d’un public un réseau Wi-Fi sans avoir à faire une quelconque « déclaration préalable ». Le mode d’accès au réseau (filaire ou hertzien) autant que le nombre de personnes pouvant se connecté n’a pas d’influence tant que le réseau reste localisé. Il faut uniquement que ce public soit restreint !

## Puissance des canaux - Pire

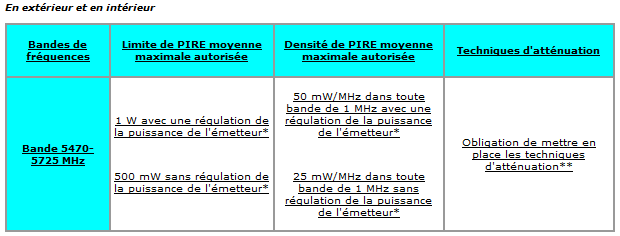
Tout cela est réglementé bien évidemment par l’Arcep…"*Il résulte de la limitation sur la puissance (PIRE) que l’étendue d’un réseau constitué au moyen de la seule technologie RLAN est typiquement de quelques centaines de mètres. L'opérateur qui souhaite déployer des liaisons point à point, avec des portées non compatibles avec les limitations de puissance indiquées dans les tableaux, doit solliciter à cet effet auprès de l'Autorité une autorisation d'utilisation de fréquences dans l'une des bandes de fréquences identifiées pour cet usage*"

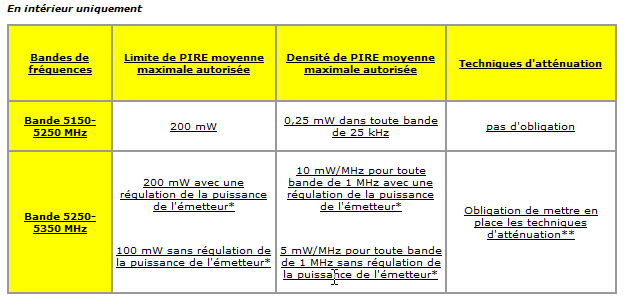
Les puissances sont exprimées en **PIRE** : **puissance isotrope rayonnée équivalente**

**Sur la bande des 2.4 Ghz**

****

**Sur la bande des 5 Ghz**

****



## Obligation "légales"

Que l'on soit déclaré ou non, tout réseau WIFI accessible au Public doit normalement respecter un certain nombre d'obligations

L’accès Internet est, en France, est soumis à un cadre précis :

* identification de l’utilisateur (assez controversé)
* conservation temporaires de ses données de connexion (obligatoire)
* filtrage des contenus illicites (tres controversé)

font partie des principales règles à mettre en place. Sans ce passage obligé, les entreprises se mettent en porte-à-faux avec la loi.

* identification de l’utilisateur (non obligatoire)

La contrainte de traçabilité des usagers pourrait faire croire à la nécessitée d'imposer l’identification de chaque utilisateur (par exemple, par un identifiant et un mot de passe associé), avant tout accès

mais, le décret du 24 mars 2006 n’a pas retenu l’hypothèse consistant à demander aux exploitants de « cybercafés », d’hôtels ou de bars qui offrent une connexion Wi-Fi, de relever l’identité de leurs clients. Il prévoit seulement la conservation des « données permettant l’identification ». Il s’agit donc, pour ces « fournisseurs de Wi-Fi » de recueillir des informations qui, mises bout à bout, constituent un faisceau d’indices permettant l’identification

* conservation temporaires de ses données de connexion (obligatoire)

Les organismes qui mettent à disposition du public un service de libre accès à internet (postes informatiques, wi-fi, etc.) sont considérés comme opérateurs de communications électroniques (OCE) et sont soumis aux obligations prévues àl'article L. 34‑1 du code des postes et des communications électroniques(CPCE). A ce titre, ils doivent conserver les données de trafic répondant aux " besoins de la recherche, de la constatation et de la poursuite des infractions pénales " et destinées aux autorités légalement habilitées.

La plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie.

Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement (Article R. 10-13 du Code des postes et des communications électroniques)

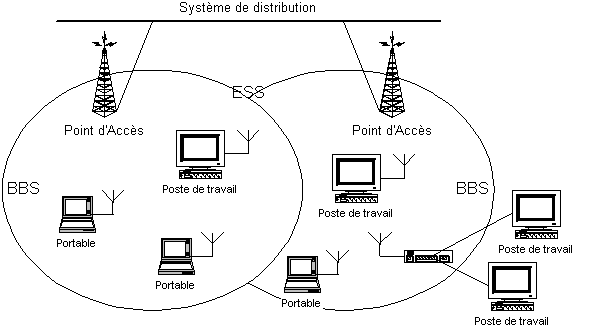
* filtrage des contenus illicites (aucune obligation)

# Les Liaisons Wi-Fi

## Structure des liaisons:

En 1998, la norme **802.11** est finalisée, et est rapidement rebaptisée **Wi-Fi (Wireless fidelity**). Un organisme, la **WECA (Wireless Ethernet Compatibility Alliance)**, s’est donné la mission de certifier l’inter-opérabilité des produits avec la norme 802.11b

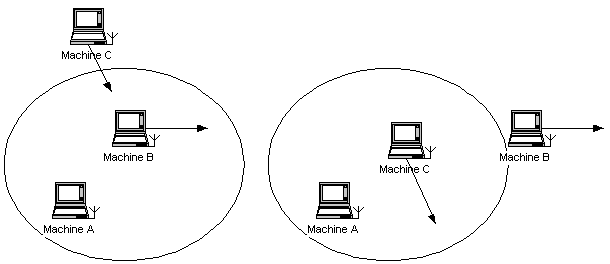
Cette norme est basée sur une architecture cellulaire (le système est subdivisé en cellules), et où chaque cellule (appelée **Basic Service Set** ou **BSS** dans la nomenclature 802.11), est contrôlée par une station de base (appelée **Access Point** ou **AP**, Point d’Accès en français).



deux modes principaux de fonctionnement existent pour les liaisons sans fils.

### Fonctionnement "AD-HOC" (IBSS):

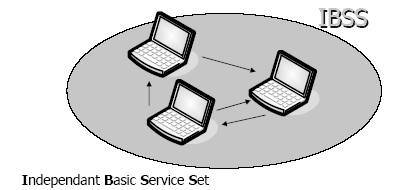
Un réseau **Ad Hoc** est un réseau où il n'y a pas d'infrastructures fixes.



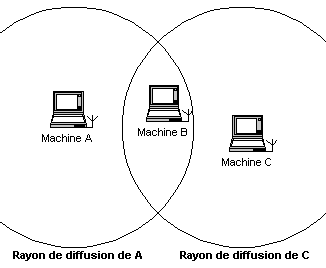
Le signal est transmis par l'intermédiaire des mobiles présents et routé dynamiquement. Une partie de ses fonctionnalités sont reprises par les stations elles-mêmes mais alors certaines fonctions ne sont pas utilisables (comme le mode d’économie d’énergie).

Ceci peut permettre le transfert de fichiers entre deux utilisateurs..

on parle aussi de **Mode IBSS**



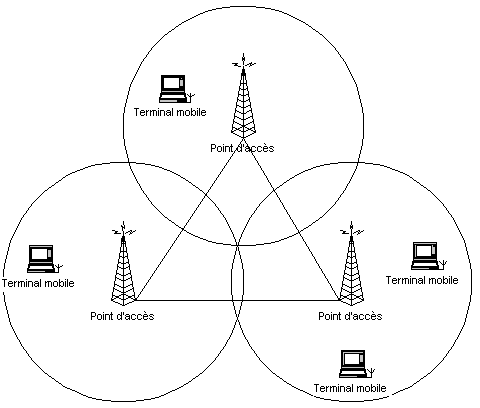
Dans une connexion ad hoc, il n’y a pas de possibilité de transfert entre les machines distantes, autres que les deux qui ont initié la communication.



Dans le schéma ci-dessus, la machine A peut dialoguer avec la machine B, mais pas avec la machine C

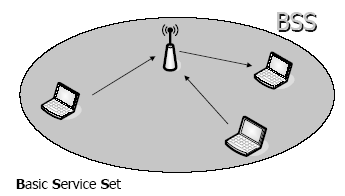
### Fonctionnement "Infrastructure":

Le mode **infrastructure** fait appel a une ou plusieurs bornes de concentration appelées **Points d’Accès**, qui gère l’ensemble des communications dans une même zone géographique.

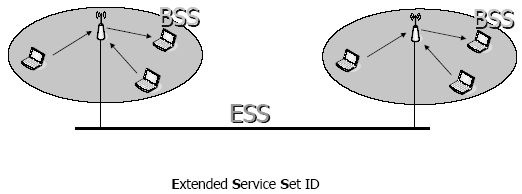


Les bornes sont connectées entre elles par une liaison ou un réseau filaire ou hertzien.

on parle aussi de **Mode IBSS**



On parle également de points d'accès en mode "Pont" voire **Mode ESS**



### Comment une station rejoint-elle une cellule existante ?

Quand une station veut accéder a un **BSS** existant (soit après un allumage, un mode veille, ou simplement en entrant géographiquement dans la zone de couverture de la cellule), la station a besoin d’informations de synchronisation de la part du Point d’Accès.

La station peut avoir ces informations par un des deux moyens suivants :

* 1. **Ecoute passive** : dans ce cas, la station attend simplement de recevoir une trame balise (**Beacon Frame**). La trame balise est une trame envoyée périodiquement par le Point d’Accès contenant les informations de synchronisation.
  2. **Ecoute active** : dans ce cas, la station essaie de trouver un Point d’Accès en transmettant une trame de demande d’enquête (**Probe Request Frame**) et attend la réponse d’enquête du Point d’Accès.

Ces deux méthodes sont valables et peuvent être choisies en fonction des performances ou de la consommation engendrées par l’échange, en terme d’énergie.

### Le processus d’authentification

Une fois qu’une station a trouvé un Point d’Accès et a décidé de rejoindre une cellule (BSS), le processus d’authentification s’enclenche. Celui-ci consiste en l’échange d’informations entre le Point d’Accès et la station, où chacun des deux partis prouve son identité par la connaissance d’un certain mot de passe.

### Le processus d’association - réassociation

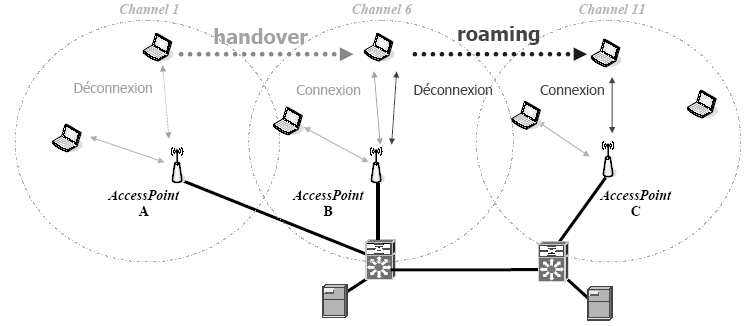
Une fois la station authentifiée, le processus d’association s’enclenche. Celui-ci consiste en un échange d’informations sur les différentes stations et les capacités de la cellule, et autorise le DSS (les Points d’Accès enregistre la position actuelle de la station). Seulement après le processus d’association, la station peut transmettre et recevoir des trames de données.

La réassociation peut survenir à cause d'éloignement grandissant, ou de gestion de la répartition de charge.

### Le roaming- handover

Les terminaux BSS peuvent se déplacer au sein de la cellule et garder une liaison directe avec le point d’accès AP, ou changer de cellule, ce qui s’appelle le **roaming**

Pour un réseau [**Wi-Fi**](http://fr.wikipedia.org/wiki/Wi-Fi), ce terme est utilisé pour évoquer le fait d'un changement de cellule ou de réseau tout en restant en communication (voix ou données). Dans ce cas il s'agit en fait plus d'un [**Handover**](http://fr.wikipedia.org/wiki/Handover) que d'un **roaming**

En TCP-IP, (qui est basé sur des paquets), la transition d’une cellule à une autre se fait entre deux transmissions de paquets, (contrairement à la téléphonie où la transition peut subvenir au cours d’une conversation.) Ceci rend le roaming plus facile en théorie, mais… les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

Le standard 802.11 ne définit pas comment le roaming est fait, mais en définit cependant les règles de base. (l’écoute active ou passive, le processus de ré-association, où une station qui passe d’un Point d’Accès à un autre sera associée au nouveau Point d’Accès).

### Sécurité

La sécurité est le premier (ou le dernier !) soucis de ceux qui déploient les réseaux locaux sans fil. Le comité de 802.11 a apporté une solution en élaborant un processus appelé **WEP** (**Wired Equivalent Privacy**).

Le principal, pour les utilisateurs, est d’être sûr qu’un intrus ne pourra pas :

**Accéder aux ressources du réseau (prévenir l’accès non authentifié)**

Ceci est obtenu en utilisant un mécanisme d’authentification où une station est obligée de prouver sa connaissance d’une clef, ce qui est similaire à la sécurité sur réseaux câblés, dans le sens où l’intrus doit entrer dans les lieux (en utilisant une clef physique) pour connecter son poste au réseau câblé.

**Capturer le trafic du réseau sans fil (Ecoute clandestine)**

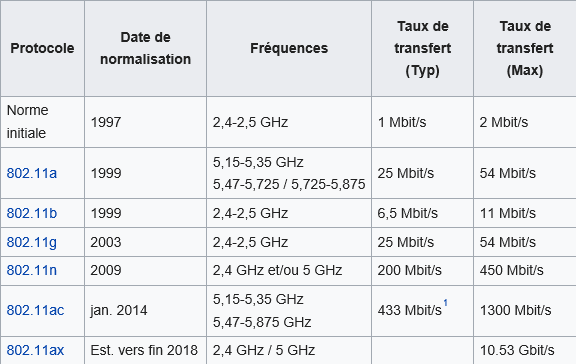
L’écoute clandestine est bloquée par l’utilisation de l’algorithme **WEP** qui est un générateur de nombres pseudo aléatoires initialisé par une clef secrète partagée. Basé sur l’algorithme RC4 de RSA (faible sécurité)

### L’économie d’énergie

Les réseaux sans fil sont généralement en relation avec des applications mobiles, et dans ce genre d’application, l’énergie de la batterie est une ressource importante. C’est pour cette raison que le standard 802.11 donne lui-même des directives pour l’économie d’énergie et définit tout un mécanisme pour permettre aux stations de se mettre en veille pendant de longues périodes sans perdre d’information. L’idée générale, est que le Point d’Accès maintient un enregistrement à jour des stations travaillant en mode d’économie d’énergie, et garde les paquets adressés à ces stations jusqu’à ce que les stations les demandent avec une **Polling Request**, ou jusqu’à ce qu’elles changent de mode de fonctionnement.

# Normes Ethernet 802.11 …

## Panels des Normes 802.11



## Les anciens 802.11a – 802.11b et 802.11g :

### 802.11b en 1999 – label WI-FI

la norme **802.11b** ou **802.11HR** (High Rate), dans la bande 2,4 GHz normalisée en septembre 1999. La technologie **DSSS** est gardée.

* Débits de 11 Mbps,
* portée de 30-50 mètres. (1 Mbps 250 m)
* Canaux disponibles (non recouvrant) : 3 parmi 13
* La Sécurité (faible) est obtenue par codage **WEP**

Une variante est connue sous la norme **802.11b+** Débits de 22 Mbps

### 802.11a en 1999

la norme **802.11a** , opérant dans la bande des 5 à 5.8 GHz, (moins encombrées que celle de 2.4Ghz) met l’accent sur l’utilisation de la technologie **OFDM** au niveau physique pour atteindre des débits plus élevés et une meilleure immunité aux interférences. Par contre il est plus sensible aux obstacles naturels et physiques(béton armé)…

* Débits de 54 Mbps
* portées de 50 mètres. !
* Canaux disponibles (non recouvrant) : 8

**N.B :** Il est donc incompatible avec les standards **802.11b et 802.11b+**

### 802.11g en 2003

la norme **802.11g**, bande 2,4 GHz et 5 GHz

* Débits de 54 Mbps
* Portée de 100 mètres.
* Canaux disponibles (non recouvrant) : 3 parmi 13
* La Sécurité est obtenue par la norme **802.i et autres 802.x**

**N.B :** Il est donc compatible avec les standards **802.11b (et 802.11b+)**

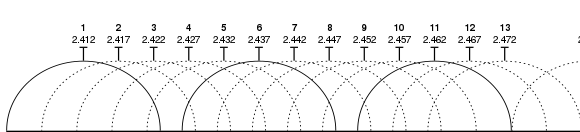
**N.B :** mais la compatibilité entre les standards **802.11b /g « coute cher »,** car il suffit qu’un seul point se connecte en b pour que la borne fasse passer son débit de 54 à 11 Mbps

### Bande 2.4 Ghz - gestion des 13 canaux 802.11b-g partage de charge

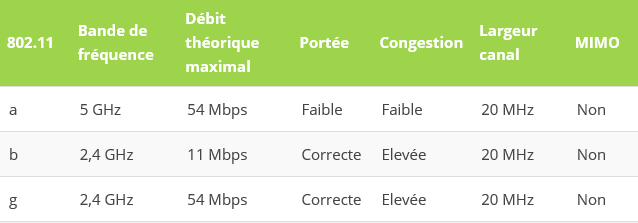
Le choix des fréquences utilisables dépends bien évidemment du pays dans lequel on se trouve, il existe à cet effet une normalisation internationale

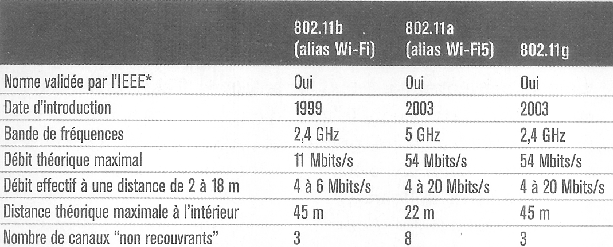
A ce propos, si le paramétrage des bornes demande toujours de choisir une régionalisation ! Cela va bien au-delà de la langue d'affichage des menus !

**N.B:** 2 Bornes avec une régionalisation différente risquent de ne pas pouvoir communiquer entre elles du fait de l'utilisation de fréquences différentes.



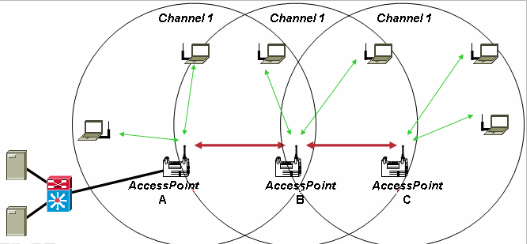
En résumé on pourrait faire le tableau suivant :





Pour optimiser la présence de différents AP pour couvrir une même zone, il faut savoir que au-delà de 3 éléments, c’est inutile (car il y aura télescopage des fréquences).

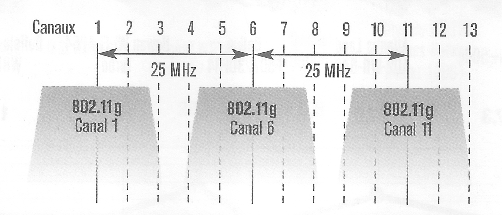
3 points d’accès en mode répéteur sur une zone de couverture partagent un débit atteignant au maximum le débit nominal d'une borne.



Mais 3 points d’accès sur une zone de couverture peuvent donner un débit atteignant de 33Mbits/s en utilisant un plan de fréquence approprié

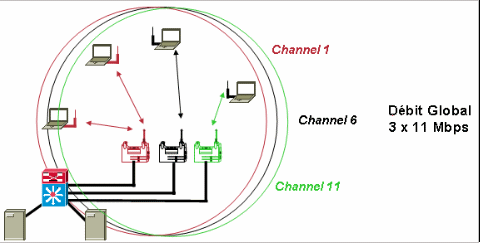
**1/6/11 – 2/7/12 – 3/8/13, et 5/10**

(Voire en France **1/5//9/13)**



Comme la fréquence du spectre d'émission en 802.11b ou g est de 22Mhz, il faut séparer les canaux d'environ 25 Mhz pour éviter les télescopages.

Permettant donc un schéma de partage de charge classique suivant



Voici un schéma de gestion fine de l’utilisation sur un niveau des 3 canaux classiques **1 – 6 - 11** :

**1 6 11**

**6 11 1 6**

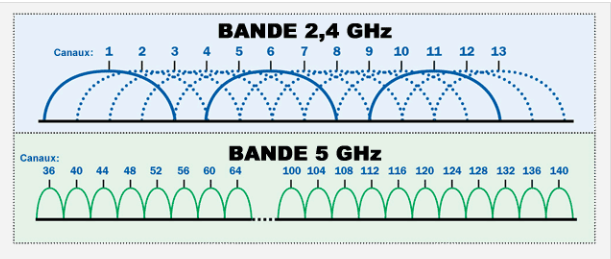
**1 6 11**

## Les nouveaux 802.11n – 802.11ac:

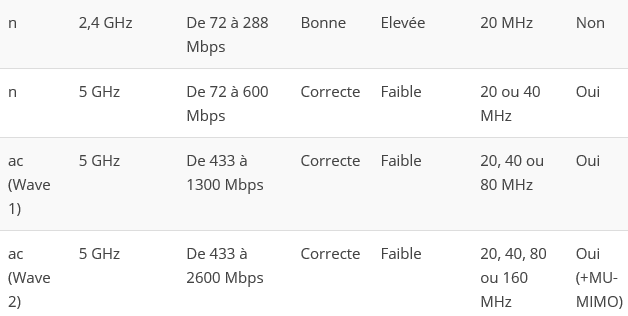
la norme **802.11n**, bande 2,4 GHz et 5 GHz

La bande (composée des 2 sous-bandes) désignée sous le nom « bande 5 GHz » et peut être utilisée par les normes Wi-Fi récentes IEEE 802.11n et IEEE 802.11ac ; la numérotation des canaux y est différente avec une numérotation « modulo 4 »

Largeur des canaux est de 44Mhz (au lieu de 25 Mhz sur la bande 2,5Ghz)







### Bande 5 Ghz - gestion des 19 canaux 802.11n-ac

**N.B :** Il est incompatible avec les standards **802.11a-b-g** précédant

* Débits de 540Mbps/100Mbps
* Portée de 50-60 mètres en intérieur.
* Canaux disponibles (non recouvrant) : 19
* Largeur des canaux de 20, 44M ou 160Mhz (au lieu de 25 MGhz sur la bande 205Ghz)
* Technologie **MIMO**

**MIMO** signifie Multiple Input Multiple Output.

Comme son nom l’indique, cette technologie permet au Wi-Fi d’exploiter simultanément plusieurs canaux. On parle par exemple de MIMO 2×2 pour deux antennes en émission et deux en réception, ce qui double le débit par rapport à une configuration sans MIMO, soit 300 Mb/s avec 40 MHz. Le

Wi-Fi N peut atteindre du MIMO 4×4, soit un maximum absolu de 600 Mb/s

Wi-Fi AC jusqu’à 8 flux en MIMO, ce qui double encore la bande passante

# Sécurité et Wi-Fi

## WEP Wired Equivalent Privacy - 802.11a - b/g

Amélioration de la sécurité en cryptant les échanges avec :

* Chiffrement **RC4**
* vecteur d’initialisation sur 24 bits
* Clé donnée au démarrage de l’échange, clé de 64 / 128 / 256 bits

## Evolution WPA – WPA2 (TKIP CCMP-AES) 802.11i

### WPA : Wireless Protection Access

En 2003 norme **WPA**, avec 2 variantes de sécurisation :

Un chiffrement **RC4** **amélioré** est utilisé, moyennant une mise à jour, la compatibilité avec les équipements précédents est assurée.

* **WPA-PSK** (Norme SOHO): associée à **TKIP,** utilisation d’une **PSK** Pre-share key, c'est-à-dire une clé partagée,
* **WPA-Enterprise** (Norme Professionnelle) : associée à **TKIP,** utilisation d’un protocole d’authentification (de mot de passe ou de certificats) Utilisation d’un serveur **RADIUS** est préconisée

### WPA 2 - 802.11i

En 2004 norme **802.11i** appelée **WPA2** avec, 2 variantes de sécurisation :

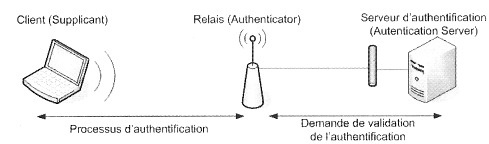
Un chiffrement **AES** est utilisé, (incompatibilité totale avec les équipements précédents. utilisant RC4)

* **WPA2-PSK** (Norme SOHO): associée à **CCMP-AES, Advanced Encryption Standard** utilisation d’une **PSK** Pre-share key, c'est-à-dire une clé partagée. (incompatibilité totale avec les équipements précédents utilisant TKIP)
* **WPA2-Enterprise** (Norme Professionnelle): associée à **CCMP-AES,** utilisation d’un protocole d’authentification selon la norme **802.1x**

|  |  |  |
| --- | --- | --- |
| **Solution** | **Protocole** | **Chiffrement** |
| WEP | WEP | RC4 |
| WPA | TKIP | RC4+ |
| WPA2 | CCMP | AES |

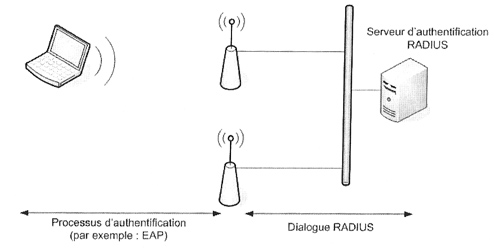
### RADIUS Remote Authentification Dial In User Service

Le processus définit trois composantes



1. Le client ou système à authentifier (**Supplicant**) souhaite se connecter au réseau
2. Le point d'accès réseau , borne WI-FI (**Authenticator**) transmet la demande auprès d'un serveur d'authentification.
3. Un serveur d'authentification valide la demande (**Authentication Server**)

Le serveur préconisé par 802.11i est un serveur RADIUS



## Mémo en 10 points :

1. Vérifier la compatibilité du matériel
2. Protection adresse MAC
3. changer les canaux par défaut
4. gérer voire limiter la puissance d'émission
5. si possible désactiver les différents modes et ne garder qu'une gamme de fréquence pour augmenter le débit
6. masquer le SSID
7. Eviter un serveur DHCP (ou faire de la réservation d'adresse)
8. Mettre une clé WEP minimum 128 Bits (correctement construite !), mieux si cryptage WPA WPA2
9. Placer les Points d'accès dehors du réseau interne, séparés par 1 firewall
10. Si nécessité de sécuriser, Mettre en place une authentification forte (serveur RADIUS), un VLAN, placer dessus un VPN voire de l'IPSEC

# Lexique WI-FI

## AES :

**Advanced Encryption Standard**

Nouvelle technique d'encryptage utilisée en WPA2 remplaçant la technique TKIP utilisée en WPA

## Adresse MAC :

Identifiant unique en hexadécimal permettant de repérer une carte réseau

## Ad-Hoc :

On parle de liaison ad-hoc lorsque deux appareils équipés de carte Wifi transmettent directement entre eux, Sans passer par un point d’accès

## Acces Point - Ap:

Voir point d’Accès

## BSS - Basic Service Set -:

Appellation anglaise de l’architecture en mode infrastructure avec un seul Point d’Accès

## DHCP :

Serveur distribuant à la demande des adresses IP préalablement déclarées. Nécessite quel client soit paramétré pour obtenir dynamiquement une adresse IP depuis le serveur DHCP, on parle alors de client DHCP.

## EAP:

**Extensible Authentication Protocol**

C’est un mécanisme d'identification universel, fréquemment utilisé dans les réseaux sans fil et les liaisons Point-A-Point. Il est obligatoire entre les liaisons AP et client

Les standards [WPA](http://fr.wikipedia.org/wiki/WPA) et [WPA2](http://fr.wikipedia.org/wiki/WPA2) ont officiellement adopté plusieurs types d’EAP comme mécanismes officiels d’identification : EAP-TLS - EAP-TTLS/MSCHAPv2 - PEAPv0/EAP-MSCHAPv2 -PEAPv1/EAP-GTC -EAP-SIM

## Egal à egal:

Voir Ad-Hoc

## ESS - Extended Service Set:

Appellation anglaise de l’architecture en mode infrastructure étendue (plusieurs points d’Accès). On parle parfois en francais de points d'accès en mode Pont.

## ESSID ou nom du réseau WIFI :

cf SSiD

## IBSS - Independant Basic Service Set:

Appellation anglaise de l’architecture mode ad hoc (sans Point d’Accès)

## MIMO - Multiple-Input Multiple-Output:

technologie utilisée pour les réseaux sans fil et permettant des transferts de données à plus longue portée et à plus grande vitesse que leWI-Fi

## Mode Infrastructure:

On parle de mode infrastructure à partir du moment ou les appareils sont reliés entre eux via des points d’accès . Selon qu’il y ait un seul ou différents points d’accès on parlera alors de mode infrastructure (IBSS), ou de mode infrastructure en mode étendu (ESS)

## Pire :

Puissance Isotrope Rayonnée Equivalente

Unité de puissance effective utilisée pour mesurer la couverture des éléments radios actif en WIFI (bornes)

## PSK :

Pre-Shared Key

Clé partagée, correspondant à la présence de 2 clé identiques sur les 2 équipements qui cherchent à communiquer.

Souvent associé à **WPA** dans l’acronyme **WPA/PSK**…

## Point d’Accès :

Appareil émetteur de fréquences sur lequel les clients wifi ont venir se connecter. En l’absence de point d’accès centralisateur, deux appareils équipés de Wifi peuvent transmettre directement entre eux, en un mode appellé ad-hoc.

## Radius Remote Authentification Dial-In User Service

Serveur d'authentification pour les accès distants

## Roaming

Action de passer de la zone de couverture d'un AP à une autre sans perdre la connexion

## SSID ou ESSID ou nom du réseau WIFI :

L'**ESSID**, souvent abrégé en **SSID**, (**Service Set Identifier)**, représente le nom du réseau et est nécessaire pour qu'une station se connecte au réseau

Se paramètre sur le poste émetteur WI-FI (dit Point d’accès).

## WEP

Wired Equivalent Privacy

Technique de cryptage apparue en 802.11b fondée sur une clé fixe donnée au démarrage de l'échange

## Wi-Fi

**Wireless fidelity**

Surnom donné à la norme 802.11en 1998. Par extension s'applique a toutes les liaisons radios qui ont suivit….

## WPA

Wired Equivalent Privacy

Technique de cryptage améliorée (postérieure à WEP ) apparue en 2003 sur 802.11g fondée sur une clé de cryptage changée à chaque trame émise

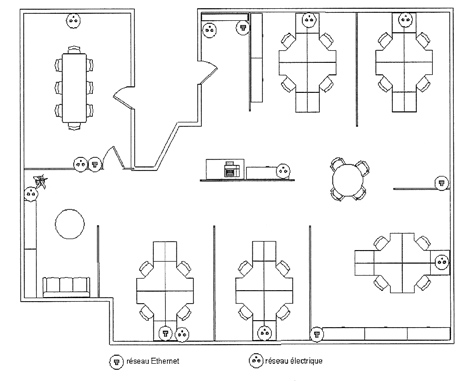
## WPA 2

Evolution du WPA introduisant une Clé cryptée plus forte AES et la présence obligatoire d'un serveur d'authentification

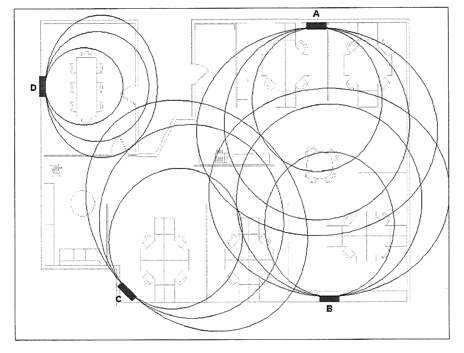
# ANNEXE

## cas pratique de gestion des canaux :

Soit un plan de bureaux de la sorte :



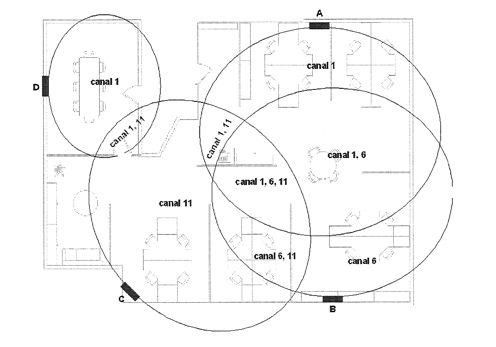
Une première approche des couvertures - puissances possibles -donnerait le schéma suivant :



Questions :

* Quels canaux choisir pour chaque Point d'accès ?
* Si le bâtiment comporte plusieurs étages "identiques", comment procéder ?

une solution pour l'étage pourrait être la suivante



S'il fallait équiper ainsi des plateaux sur plusieurs étages, comment faudrait il procéder ?

et bien pour le 1° étage, on travaille avec les fréquences

**1/6/11**

pour le 2° étage, avec les fréquences

**2/7/12**

pour le 3° étage, avec les fréquences

**3/8/13**