

TSF : Généralités 2/2

Transmission sans fils

M. BURNET

06/11/2017

<u>I. LES RESEAUX SANS FILS</u>	<u>3</u>
I. 1. REPRESENTATIONS	3
I. 2. AVANTAGES / CONTRAINTES.....	3
<u>II. CATEGORIE DE RESEAUX :.....</u>	<u>3</u>
II. 1. LE WPAN.....	3
II. 2. LE WLAN.....	4
II. 3. LE WMAN	4
II. 4. LE WWAN.....	4
II. 5. RESUME	5
<u>III. LE BLUETOOTH</u>	<u>5</u>
III. 1. CARACTERISTIQUES	5
III. 2. EVOLUTION DE LA NORME	5
III. 3. ROBUSTESSE DU BLUETOOTH.....	6
III. 4. PROTOCOLE D'ECHANGE DE DONNEES BLUETOOTH	6
III. 5. DES FAILLES DANS LA SECURITE	6
<u>IV. LE WIFI</u>	<u>7</u>
IV. 1. CARACTERISTIQUES	7
IV. 2. BANDE DE FREQUENCES ET COHABITATION	7
IV. 3. REPARTITION DES CANAUX	8
IV. 4. REPARTITION SPECTRALE	8
IV. 5. TOPOLOGIE INFRASTRUCTURE.....	8
IV. 6. TOPOLOGIE AD-HOC	9
IV. 7. NOTION DE ROAMING	10
<u>V. LE ZIGBEE.....</u>	<u>10</u>
V. 1. CARACTERISTIQUES	10
V. 2. TOPOLOGIE	11
<u>VI. LE BLE.....</u>	<u>11</u>
<u>VII. COMPARATIF ZIGBEE / BLE.....</u>	<u>11</u>

I. Les réseaux sans fils

I. 1. Représentations

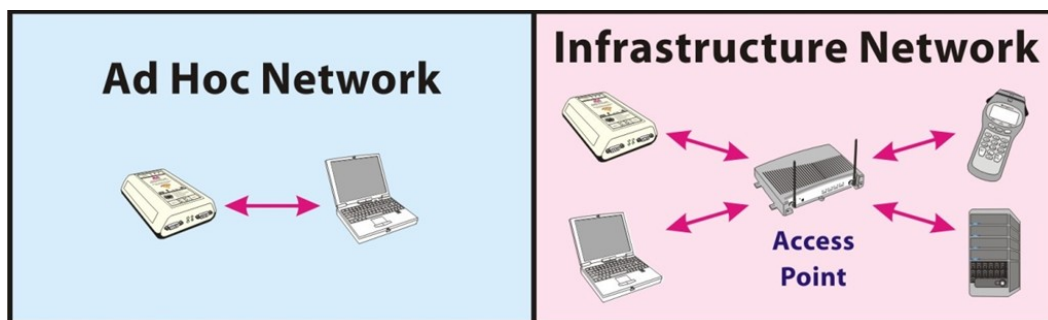
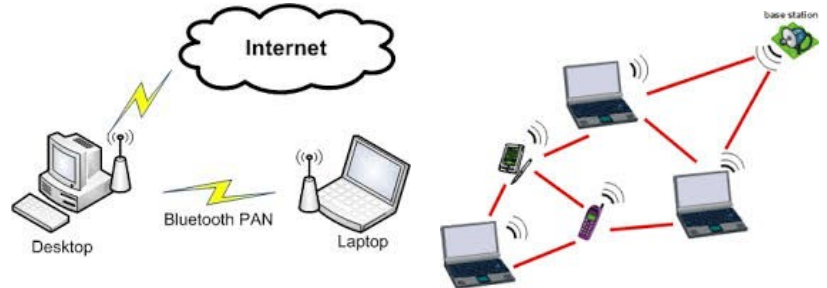
Un réseau sans fils est réseau dans lequel au moins 2 terminaux peuvent communiquer sans liaison filaire.

Mobilité : possibilité qu'à un utilisateur de rester connecté tout en se déplaçant.

Support : ondes radio ou infrarouges.

Différentes technologies selon :

- la fréquence d'émission
- le débit
- la portée des transmissions
- les besoins de sécurité



I. 2. Avantages / Contraintes

Avantages

- Facilité de déploiement
- Interopérabilité avec les réseaux filaires
- Grande souplesse
- Non destructif
- Grande mobilité
- Coût

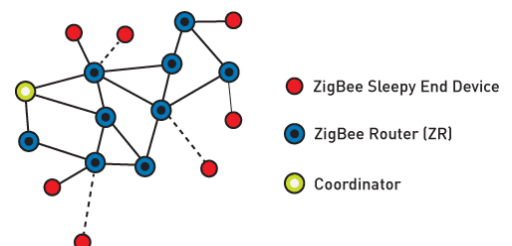
Contraintes :

- Sensibilité aux interférences
- Confidentialité des données.
- Réglementation
- Débit inférieur au filaire et à partager
- Aspects sanitaires

II. Catégorie de réseaux :

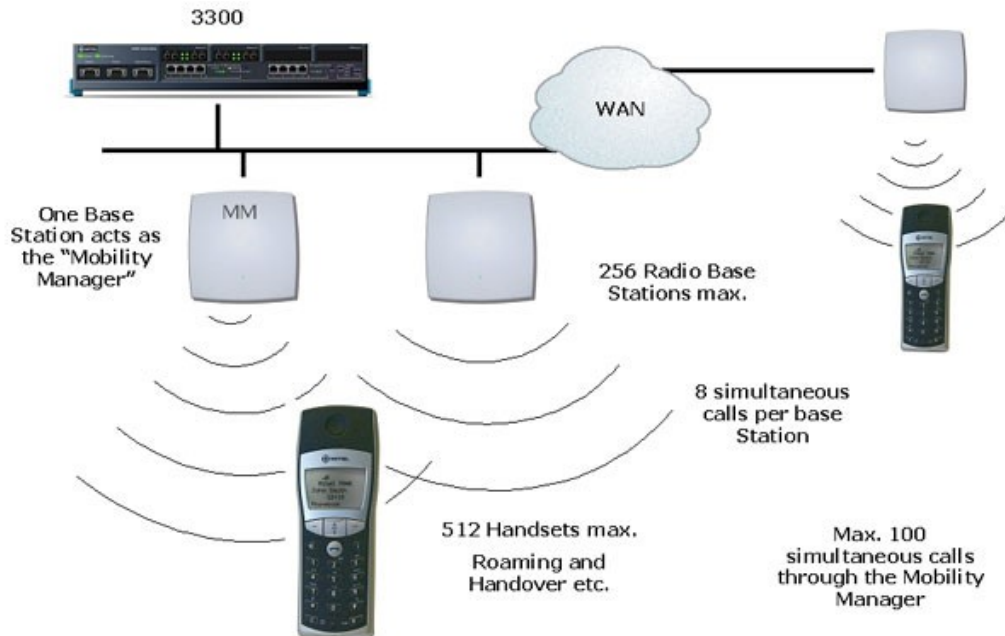
II. 1. Le WPAN

- WPAN = Wireless Personal Area Network
→ faible portée : quelques dizaines de mètres
- Technologies :
→ Bluetooth (IEEE 802.15.1)
→ Zigbee (IEEE 802.15.4 ; 250kbps)
→ Infrarouges



II. 2. Le WLAN

- WLAN = Wireless Local Area Network
→ portée : une à plusieurs centaines de mètres
- Technologies :
 - Wifi (IEEE 802.11 (a/b/c/g))
 - HiperLan2 (54Mbps ; bande 5,4GHz – 5,7GHz)
 - DECT (32kbps à 384kbps ; bande 1,88GHz - 1,9GHz)



II. 3. Le WMAN

- WMAN = Wireless Metropolitan Area Network
→ portée : quelques kilomètres
- Technologies :
 - WiMax (IEEE 802.16e : 30Mbps : bande 2GHz - 6GHz)
 - ETSI HiperMan (bande 2GHz - 11GHz)

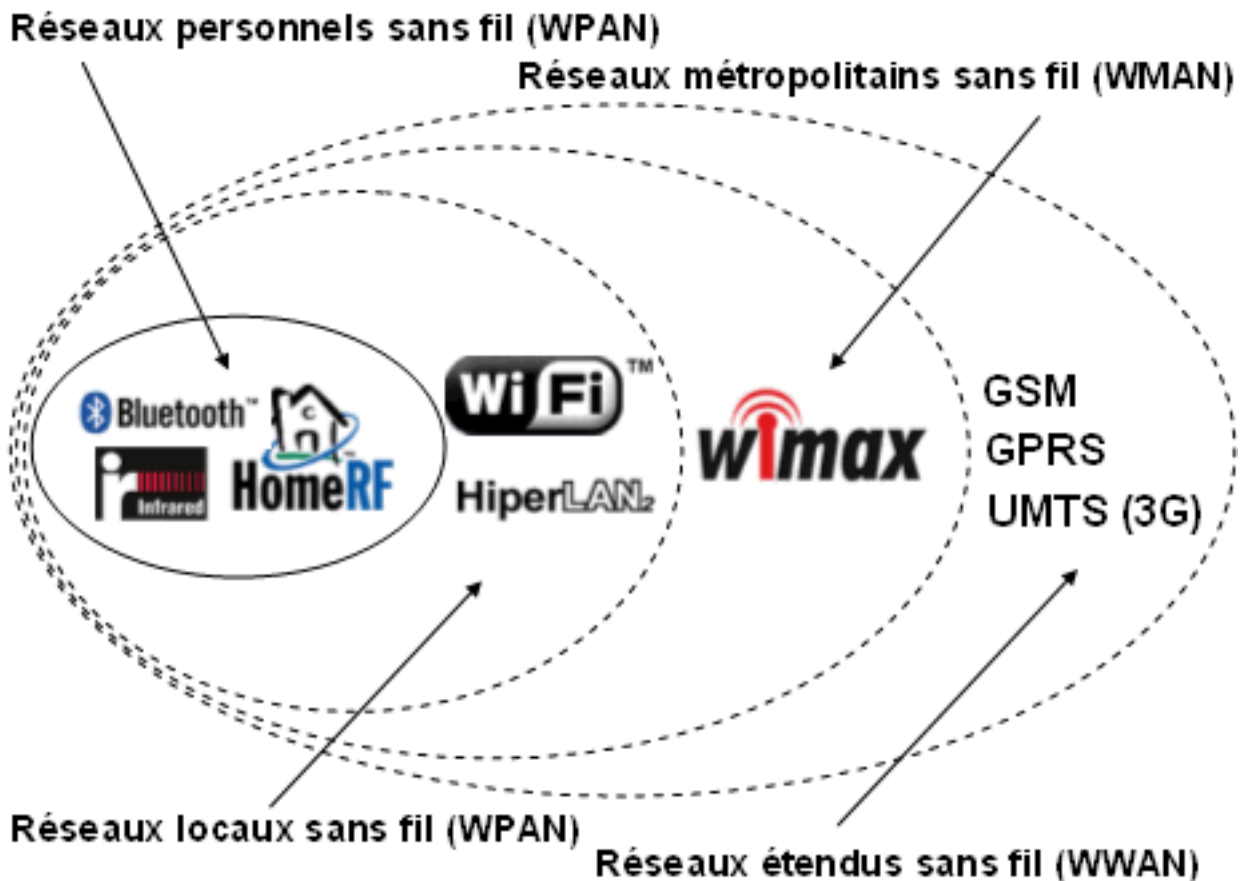


II. 4. Le WWAN

- WWAN = Wireless Wide Area Network
→ portée : plusieurs centaines de kilomètres
→ réseaux cellulaires mobiles
- Technologies :
 - GSM 900 (bande 880-915 MHz pour l'envoi de la voix ou des données depuis le mobile, bande 925-960 MHz pour la réception des informations venant du réseau)
 - GSM 1800
 - GPRS ou 2.5G (extension du GSM : 50kbps max)
 - UMTS ou 3G (144 kbps pour une utilisation mobile en mouvement rapide, 384 kbps pour une utilisation piétonne)
 - LTE ou 4G (débit pratique : 60Mbps)
 - LTE-A ou 4G+ (de 10 à 450Mbps descendant, 5 à 100Mbps montant)



II. 5. Résumé



III. Le Bluetooth

III. 1. Caractéristiques

Créé en 1994 par Ericsson

Débit : 100Mbps

Très faible consommation d'énergie

Faible portée

Utilisation : échanger une faible quantité de données sur une courte distance

Bande de fréquences ISM entre 2 401,5 et 2 480,5 MHz.
→ pas de licence

79 canaux RF séparés par 1 MHz

Nombre maximal d'appariements :
→ 65535



III. 2. évolution de la norme

Bluetooth V1.0 : apparition en 1999

Bluetooth v1.1 normalisé en 2002 sous le nom IEEE 802.15.1-2002

Bluetooth v4.1, rendue publique en 2013

Classe	Puissance	Portée
1	100 mW (20 dBm)	100 mètres
2	2,5 mW (4 dBm)	10 à 20 mètres
3	1 mW (0 dBm)	Quelques mètres

III. 3. Robustesse du Bluetooth

La technologie Bluetooth utilise une méthode de transmission de signaux par ondes radio qui utilise plusieurs canaux (sous-porteuses) répartis dans une bande de fréquence selon une séquence pseudo-aléatoire connue de l'émetteur et du récepteur.

→ FHSS ou Frequency Hopping Spread Spectrum

On parle d'étalement de spectre par saut de fréquences (1600 sauts par seconde).

Avantages :

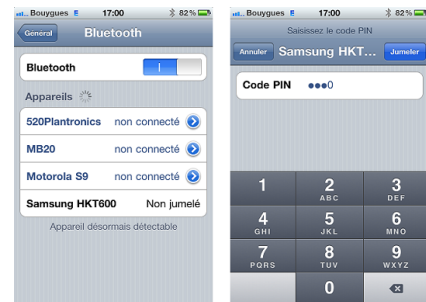
- très résistant aux interférences,
- signal difficile à intercepter,
- partage des bandes de fréquence avec d'autres types de transmission



III. 4. Protocole d'échange de données Bluetooth

L'appariement (pairing en anglais) : les deux objets doivent se reconnaître comme étant équipés de la technologie Bluetooth.

- accord pour être maître ou esclave.
- un code PIN est donné par le propriétaire.
- calcul d'une clé d'échange provisoire.
- vérification mutuelle du code PIN
- création d'une clé d'authentification commune



Après appariement, les objets partagent la même clé d'authentification.

Après séparation, ils doivent s'authentifier l'un à l'autre.

- Le maître transmet un nombre aléatoire.
- Le maître et l'esclave suivent un algorithme de calcul utilisant ce nombre et la clé d'authentification.
- L'esclave envoie la valeur calculée.
- Si la valeur calculée par le maître est identique à celle émise par l'esclave alors la procédure est effectuée dans l'autre sens..

L'échange de données peut alors reprendre.



Une fois qu'ils se sont authentifiés, les deux appareils s'échangent une clé de communication, générée par un algorithme à partir de la clé d'authentification et d'une valeur aléatoire. Les données envoyées sont chiffrées ensuite à l'aide d'un algorithme de chiffrement.

III. 5. Des failles dans la sécurité

La sécurité du Bluetooth dépend pour beaucoup de la phase d'authentification.

Problème : Par exemple, une oreillette n'a pas de clavier pour rentrer un code PIN. Dans ce cas, l'oreillette impose d'utiliser un code PIN fixé en usine, qui est souvent 0000 ou 1234 !

→ Certains produits bas de gamme imposent une clé d'authentification fixe.

IV. Le WiFi

IV. 1. Caractéristiques

Wi-Fi → Wireless Fidelity (noté WiFi à tort).

Nom donné à la certification délivrée par la Wi-Fi Alliance.

Norme initiale : 802.11 (publiée en 1997)

802.11b la plus répandue : 11 Mbps

300m en champ libre

13 canaux dans la bande des 2.4GHz

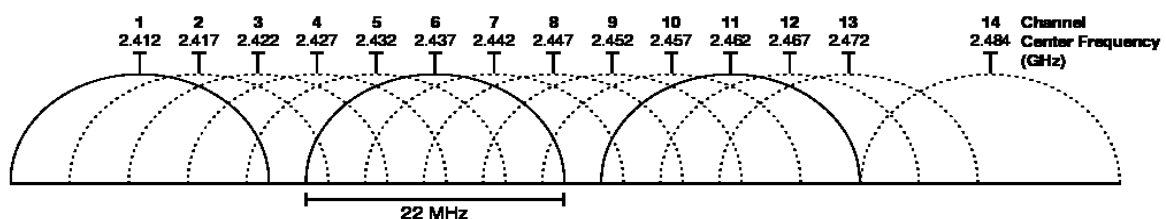
17 déclinaisons de la norme 802.11 existent....

→ exemple : 802.11g (haut débit :54 Mbps théoriques 25 Mbps réels)



IV. 2. Bande de fréquences et cohabitation

- Puissance typique : 20 dBm
- Portée typique : rayon de 100m
- Plage opérationnelle 802.11b: 2,4 à 2,4835GHz
- 13 canaux répartis tous les 5 MHz (Europe)
- Canaux 1 à 8 partagés avec les radioamateurs
- Canaux 1, 5, 9, 13 : caméras sans fil
- 2,450 GHz → four à micro-ondes



IV. 3. Répartition des canaux

PHY (MHz)	Frequency Band (MHz)	Geographical Region	Modulation	Channels	Bit rate (Mbps)	Typical Output Power (dBm)
2450	2401-2483	Europe* Japan	DBPSK DQPSK	13	1, 2, 5.5, 11	20
	2401-2473	United States, Canada		11		
	2446-2483	France		4		
	2446-2473	Spain		2		

* Excluding France and Spain

Table 2: IEEE 802.11b Frequency Bands and Data Rates

IV. 4. Répartition spectrale

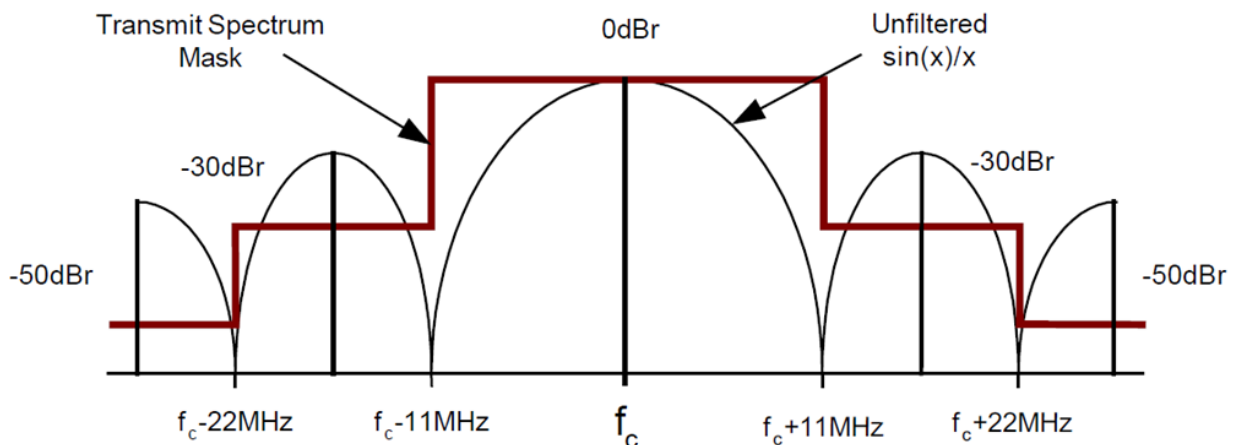


Figure 1: 802.11b Spectral Mask

La forme du spectre est liée aux types de modulation employés

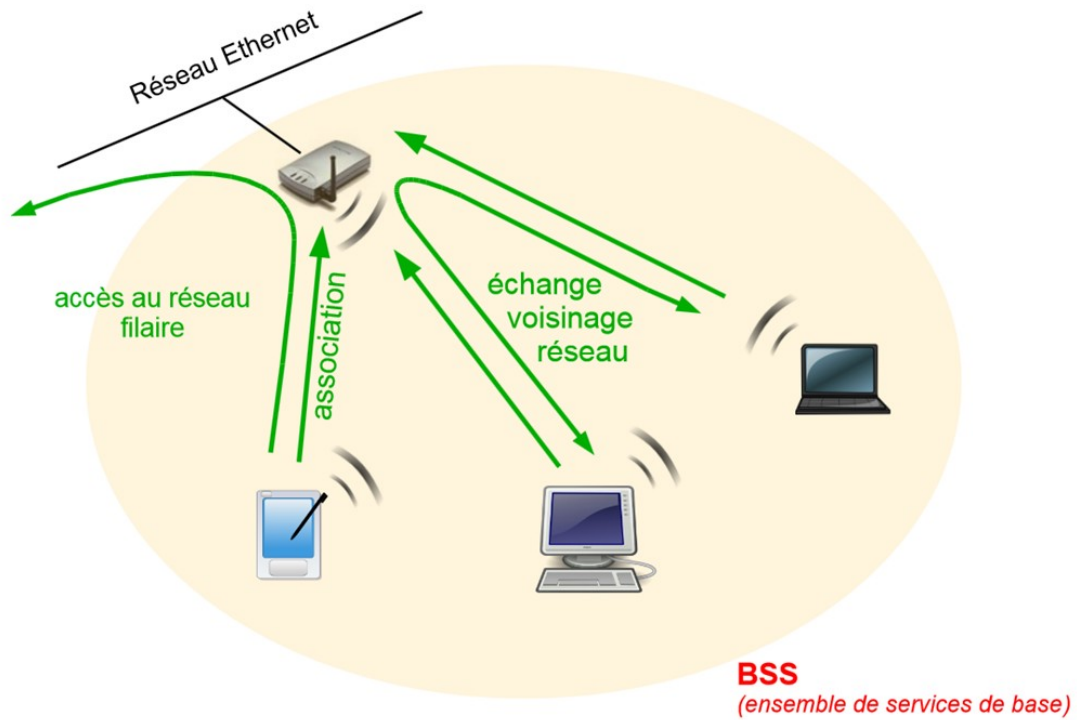
- DBPSK = Differential Binary phase-shift keying
- DQPSK = Differential Quadrature phase-shift keying

IV. 5. Topologie Infrastructure

Chaque station se connecte à un point d'accès.

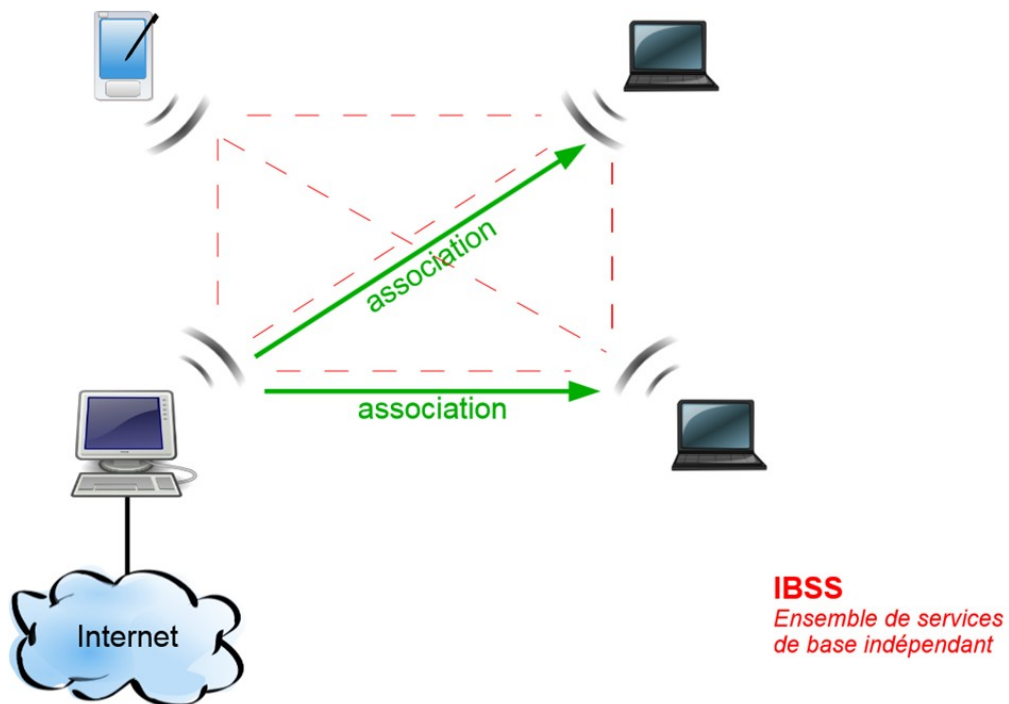
- association et ev. authentification
- connexion à la ressource Ethernet (bridge IP)
- communication avec les autres stations (IP)

A un point d'accès peuvent être associées jusqu'à 100 stations

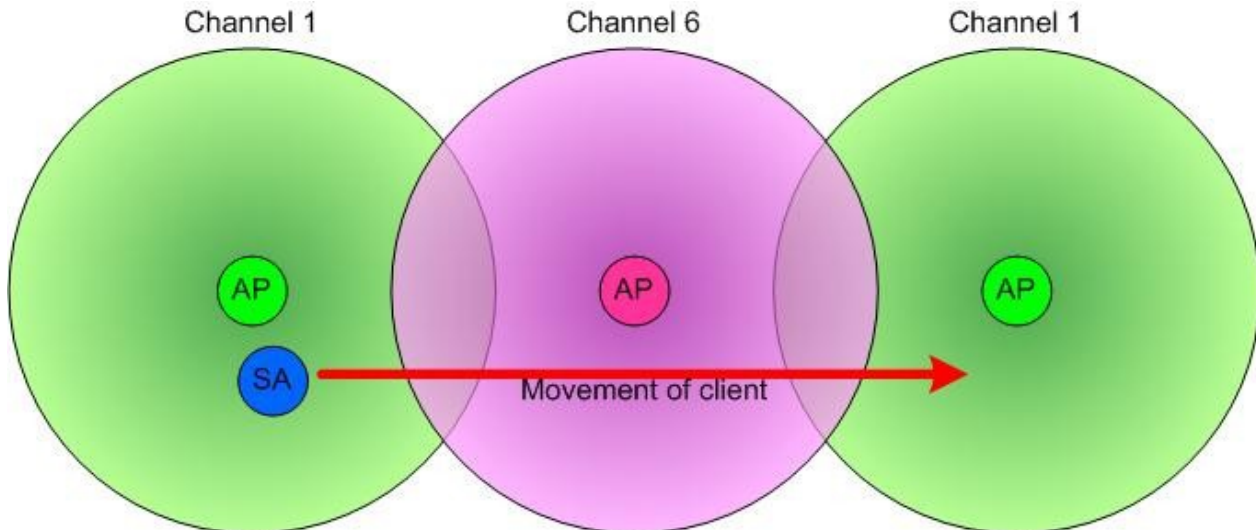


IV. 6. Topologie ad-hoc

Chaque adaptateur joue successivement le rôle de Point d'Accès (Access Point) et de client. Les machines communiquent ensemble en point à point (peer to peer)



IV. 7. Notion de Roaming



En fonction de l'organisation spatiale des canaux, un service continu en mobilité peut être offert : c'est le roaming (802.11f).

V. Le ZigBee

V. 1. Caractéristiques

Protocole basé sur la norme IEEE 802.15.4

Spécifications ratifiées en décembre 2004

Protocole simplifié par rapport à Bluetooth

→ moins de code → moins de besoin mémoire

Faible consommation → meilleure autonomie

Nombre de nœuds (device) max : 2^{16}

Débit : 250kbps

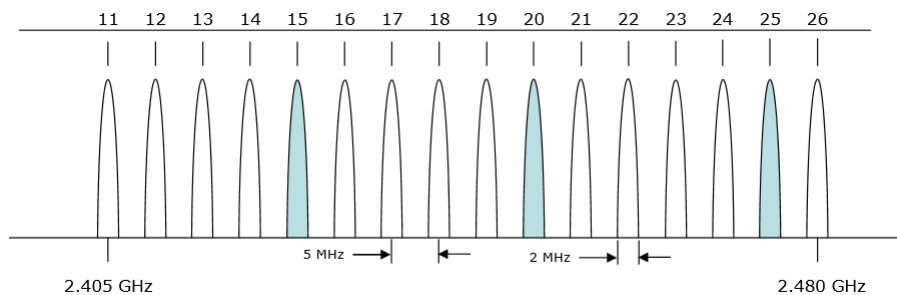
Portée : $\approx 100\text{m}$

Porteuses / Nb Canaux :

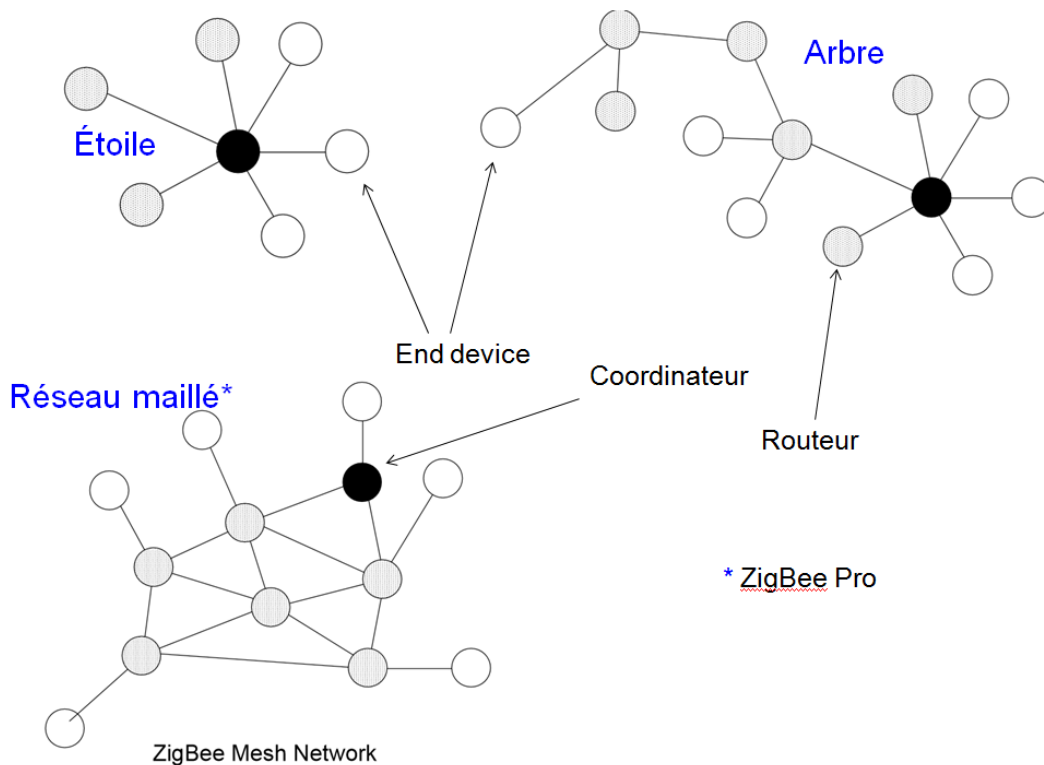
→ 868 MHz / 1 (Europe)

→ 915 MHz / 10 (US)

→ 2.4 GHz / 16 (monde)



V. 2. Topologie

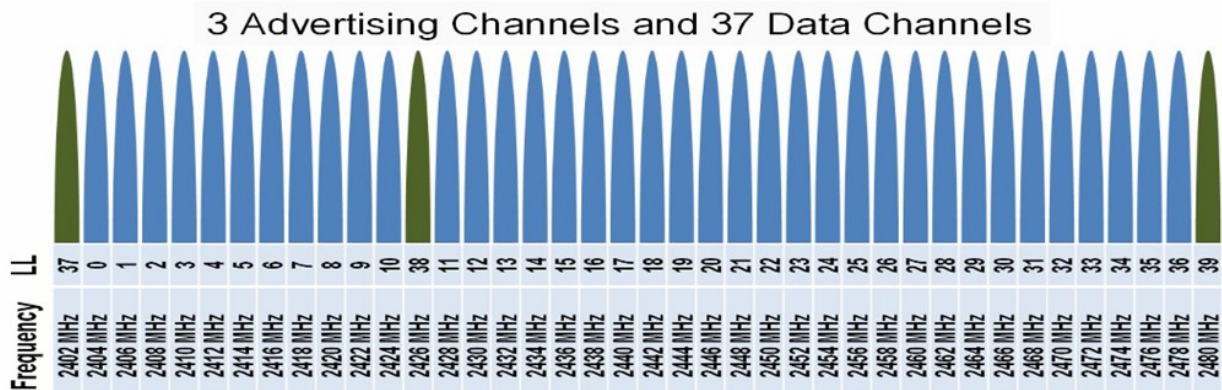


VI. Le BLE

BLE = Bluetooth Low Energy (autre nom : Wibree)

ULP : Ultra Low Power → optimisé pour une pile CR2032

40 canaux occupant chacun 2MHz de bande passante



Débit réel : 20 kbps → application avec faibles volumes de données à transférer.

Débit théorique : 1Mbps (GFSK)

Jusqu'à 16 millions de noeuds dans un réseau

VII. Comparatif ZigBee / BLE

Problème de connectivité : ZigBee n'est pas implanté dans les ordinateurs ou les téléphones mobiles

ZigBee est en avance dans le développement d'applications domotiques mais BLE s'impose dans la téléphonie mobile, l'automobile, l'industrie du PC...

Interopérabilité ? Capacité que possède un produit ou un système à fonctionner avec d'autres produits ou systèmes existants ou futurs sans restriction d'accès ou de mise en œuvre.

→ les protocoles couches hautes de BLE ne sont pas identiques à ceux de Bluetooth

→ des puces (CSR8xxx) sont disponibles acceptant de fonctionner dans les deux modes.