Pascal Ciurlik
Nicolas Engrand
Sébastien Marszalek
Xavier Okoué

WIFI
&
BLUETOOTH

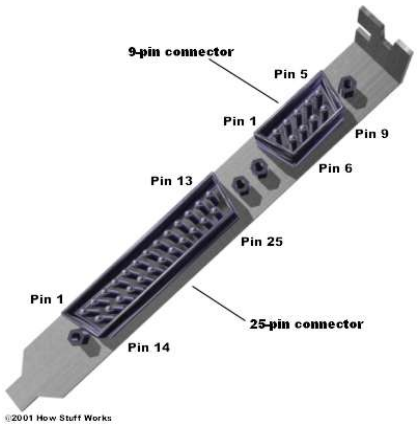
USTL

SOMMAIRE

BLUETOOTH

I- Le Bluetooth, une évolution du port série

Afin de relier des périphériques à un ordinateur, le port série ou RS232 fut inventé dans les années 60. Il a été énormément utilisé et est encore présent aujourd'hui sur les cartes mères, notamment pour relier les claviers et souris.



Le gros désavantage du port série est qu'il ne permet de relier qu'un seul périphérique à la fois. Son utilisation est aussi limitée puisque le branchement d'un port série ne se fait que l'ordinateur éteint. Pour corriger ses différents problèmes, on a inventé le port USB (Universal Serial Bus)

Bluetooth est une évolution de ce port USB, mais sans fil.

« Bluetooth » se traduit en anglais par « dent bleue » qui était le surnom du roi danois Harald II (910-986) qui unifia la Suède et la Norvège et introduisit le christianisme dans les pays scandinaves. Pourquoi une référence à une personnalité scandinave pour cette technologie ? tout simplement parce que le Bluetooth a été inventé par l'entreprise suédoise Ericsson en 1994.

Un groupe d'intérêt baptisé Bluetooth SIG (Special Interest Group) a été formé afin de produire les spécifications Bluetooth 1.0. Ce groupe réunissait plus de 2000 entreprises telles que Ericsson, IBM, Intel, Microsoft, Motorola, Nokia et Toshiba…

II- Caractéristiques

Le monde « sans fil » utilise deux concepts bien distincts :

- la technologie IrDA, principale concurrente du Bluetooth, utilise les rayons lumineux pour les transmissions de données (infrarouges). Elle est utilisée par exemple pour les télécommandes et certains téléphones portables. Principal inconvénient : les infrarouges ne peuvent traverser les objets et les appareils à relier doivent donc être en contact visuel.

- La technologie Bluetooth utilise les ondes radio (bande de fréquence des 2.4 GHz) et permet à deux appareils situés dans deux pièces différentes de se relier. La portée est limitée à 100 m et diminue suivant les obstacles rencontrés (murs, etc…)

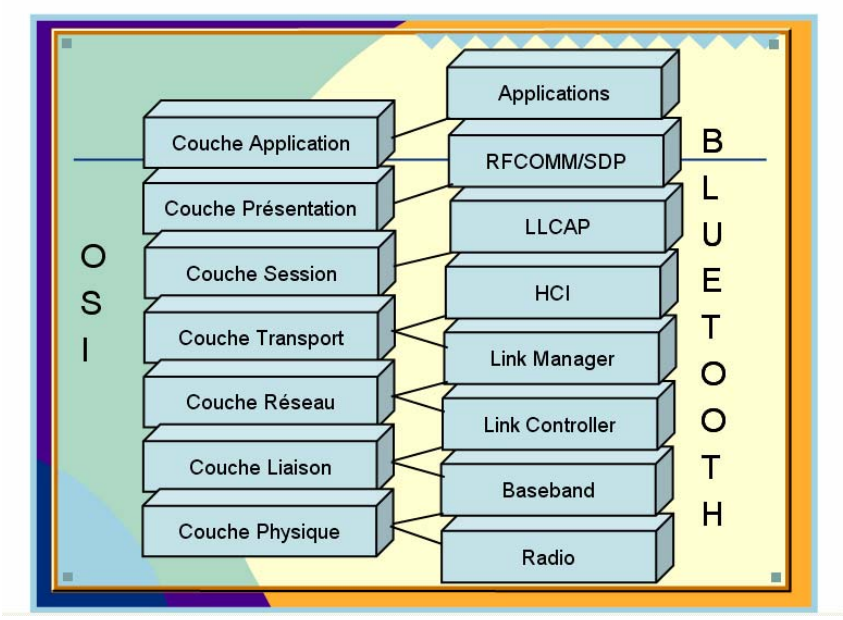
Les normes Bluetooth

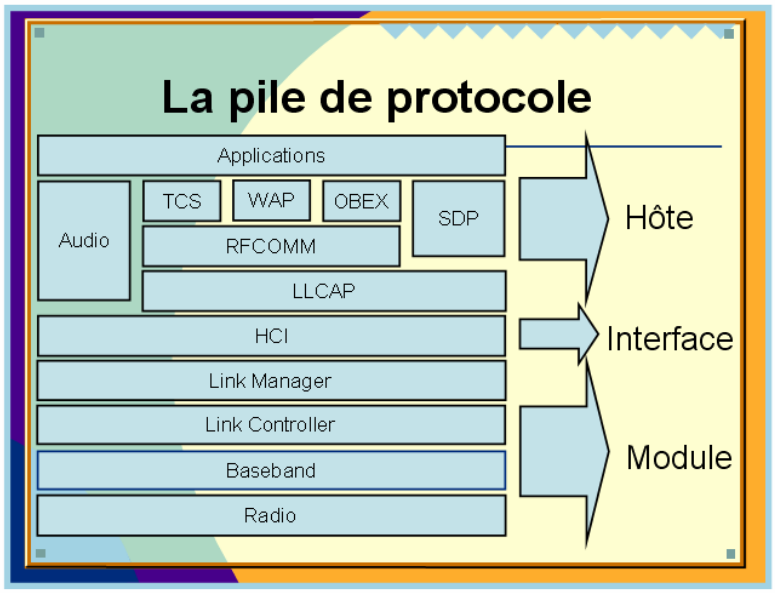
Bluetooth a été déposé à l'IEEE (Institute of Electrical and Electronic Engineers)

- IEEE 802.15.1 standard Bluetooth, debit de 1Mbit/sec (1600 échanges par seconde en full-duplex), Bluetooth v1.x
- IEEE 802.15.2 recommandations pour l'utilisation de la bande de fréquence des 2.4 GHz, pas encore validé
- IEEE 802.15.3 standard en cours de développement pour le haut débit (plus de 20 Mb/s)
- IEEE 802.15.4 standard en cours de développement pour le bas débit

Protocoles Bluetooth

Comme tout réseaux, la technologie bluetooth peut être décrite avec une notion de couche mais son modèle est différent du modèle OSI. On parle de piles de protocoles.





Pour nos explications, nous allons séparer la pile de protocoles en deux, une couche physique (appelée aussi hôte) et la couche applicative (appelée aussi module). C'est le HCI (Host Interface Controler) qui fera le lien entre le matériel et le logiciel.

III- Spécifications techniques

1- Présentation de la couche physique

Les éléments fondamentaux d'un produit Bluetooth sont définis dans les deux premières couches protocolaires, la couche radio et la couche BaseBand. Ces couches prennent en charge les tâches matérielles comme le contrôle du saut de fréquence et la synchronisation des horloges.

a) La couche radio fréquence (RF)

La couche radio (la couche la plus basse) est gérée au niveau *matériel*. C'est elle qui s'occupe de l'émission et de la réception des ondes radio. Elle définit les caractéristiques telles que la bande de fréquence et l'arrangement des canaux, les caractéristiques du transmetteur, de la modulation, du receveur, etc.
La technologie Bluetooth utilise l'une des bandes de fréquences ISM (Industrial, Scientific & Medical) réservée pour l'industrie, la science et la médecine. La bande de fréquences utilisée est disponible au niveau mondial et s'étend sur 83,5 MHz (de 2,4 à 2,4835 GHz).
Cette bande est divisée en 79 canaux (23 en France) séparés de 1 MHz.
Le codage de l'information se fait par sauts de fréquence.
La période est de 625µs ce qui permet 1600 sauts par seconde.
Il existe 3 classes de modules radio Bluetooth sur le marché ayant des puissances différentes et donc des portées différentes :

Classe	Puissance	Portée
1	100 mW (20 dBm)	100 mètres
2	2,5 mW (4 dBm)	15 à 20 mètres
3	1 mW (0 dBm)	10 mètres

La plupart des fabriquants du SIG d'appareils électroniques utilisent des modules de classe 3.
Pour transmettre des datas, la technologie Bluetooth utilise le FHSS (Frequency Hopping Spread Spectrum).Le principe du FHSS est la commutation rapide entre plusieurs canaux de fréquence,utilisant un ordre pseudo aléatoire connu tant à l'émetteur qu'au récepteur pour la synchronisation. Ainsi, les équipements radio participant à une transmission utilisant FHSS doivent utiliser la même séquence de saut de fréquence pour pouvoir communiquer.

L’utilisation de FHSS dans Bluetooth permet :

- Une synchronisation parfaite entre l’émetteur et le récepteur car ils sont obligés d’utiliser la même séquence de sauts pour communiquer.
- D’émettre à plusieurs simultanément en utilisant des combinaisons de saut de fréquences différentes. Les fréquences sont ainsi partageables.
- De limiter les interférences (collisions) car les fréquences ne sont plus polluées.

b) La bande de base (baseband)

La bande de base (ou *baseband* en anglais) est également gérée au niveau matériel. C'est au niveau de la bande de base que sont définies les adresses matérielles des périphériques (équivalent à l'adresse MAC d'une carte réseau). Cette adresse est nommée *BD_ADDR* (Bluetooth Device Address) et est codée sur 48 bits. Ces adresses sont gérées par la IEEE Registration Authority.
C'est également la bande de base qui gère les différents types de communication entre les appareils. Les connexions établies entre deux appareils Bluetooth peuvent être synchrones ou asynchrones.

La bande de base peut donc gérer deux types de paquets :

- Les paquets SCO (Synchronous Connection-Orientated) Utilisés principalement pour la voix.
- Les paquets ACL (Asynchronous Connection-Less) Utililisés principalement pour des les autres type de données.

c) Le contrôleur de liaisons (Link Controller)

Cette couche gère la configuration et le contrôle de la liaison physique entre deux appareils. Le travail du controleur de lien est de commander la construction de paquets à la couche inférieur (baseband), un à un, afin d'établir et de maintenir une ligne de transmission fiable.

d) Le gestionnaire de liaisons (Link Manager)

Cette couche gère les liens entre les périphériques maîtres et esclaves (dans les réseaux Bluetooth). Il gére aussi les types de liaisons (synchrones ou asynchrones).
C'est le gestionnaire de liaisons qui implémente les mécanismes de sécurité comme :

- L'authentification,
- Le pairage,
- La création et la modification des clés,
- Et le cryptage.

e) L'interface de contrôle de l'hôte (HCI)

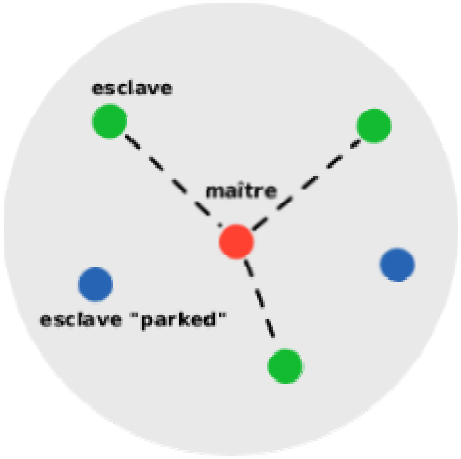
Cette couche fournit une méthode uniforme pour accéder aux couches matérielles. Son rôle de *séparation* permet un développement indépendant du *hardware* et du *software*.
Les protocoles de transport suivants sont supportés :

- USB (Universal Serial Bus)
- PC Card
- RS-232
- UART

2- Les différentes topologies de réseaux Bluetooth

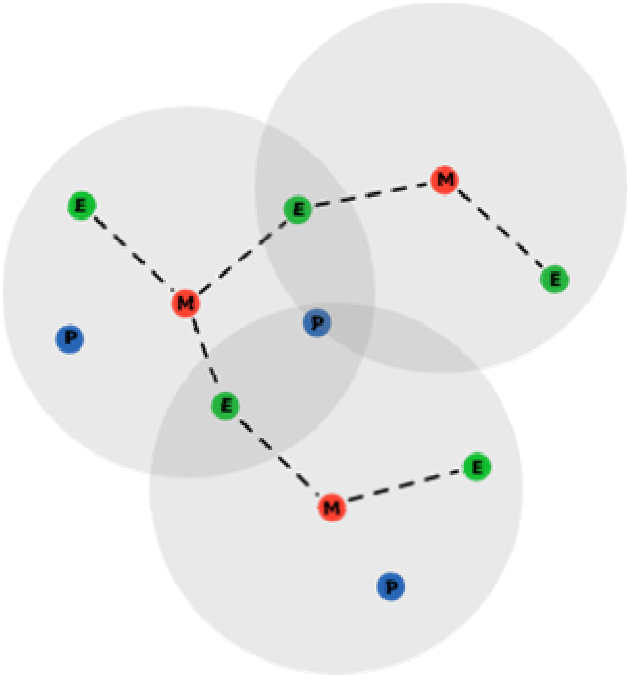
a) Réseau piconet

Un piconet est un réseau qui se crée de manière instantanée et automatique quand plusieurs périphériques Bluetooth sont dans un même rayon (10 m).
Ce réseau suit une topologie en étoile : 1 maître / plusieurs esclaves. Un périphérique maître peut administrer jusqu'à 7 esclaves actifs ou 255 esclaves en mode parked (=inactif).
La communication est directe entre le maître et un esclave. Les esclaves ne peuvent pas communiquer entre eux.
Tous les esclaves du piconet sont synchronisés sur l'horloge du maître. C'est le maître qui détermine la fréquence de saut de fréquence pour tout le piconet.



b) Réseau scatternet

Les Scatternets sont en fait des interconnexion de Piconets (Scatter = dispersion). Ces interconnexions sont possibles car les périphériques esclaves peuvent avoir plusieurs maîtres, les différents piconets peuvent donc être reliés entre eux.



3- Présentation de la couche applicative

a) La couche L2CAP

L2CAP signifie Logical Link Control & Adaptation Protocol.
Cette couche permet d'utiliser simultanément différents protocoles de niveaux supérieurs.
Un mécanisme permet d'identifier le protocole de chaque paquet envoyé pour permettre à l'appareil distant de passer le paquet au bon protocole, une fois celui-ci récupéré.(Multiplexage)
La couche L2CAP gère également la ségmentation (et le réassemblage) des paquets de protocoles de niveaux supérieurs en paquets de liaison de 64 Ko.

b) Les services

RFCOMM est un service basé sur les spécifications RS-232, qui émule des liaisons séries. Il peut notamment servir à faire passer une connexion IP par Bluetooth.

SDP siginifie *Service Discovery Protocol*. Ce protocole permet à un appareil Bluetooth de rechercher d'autres appareils et d'identifier les services disponibles. Il s'agit d'un élément particulièrement complexe de Bluetooth.

OBEX siginifie *Object Exchange*. Ce service permet de transférer des données grâce à OBEX, protocole d'échange de fichiers IrDA.

c) La couche application

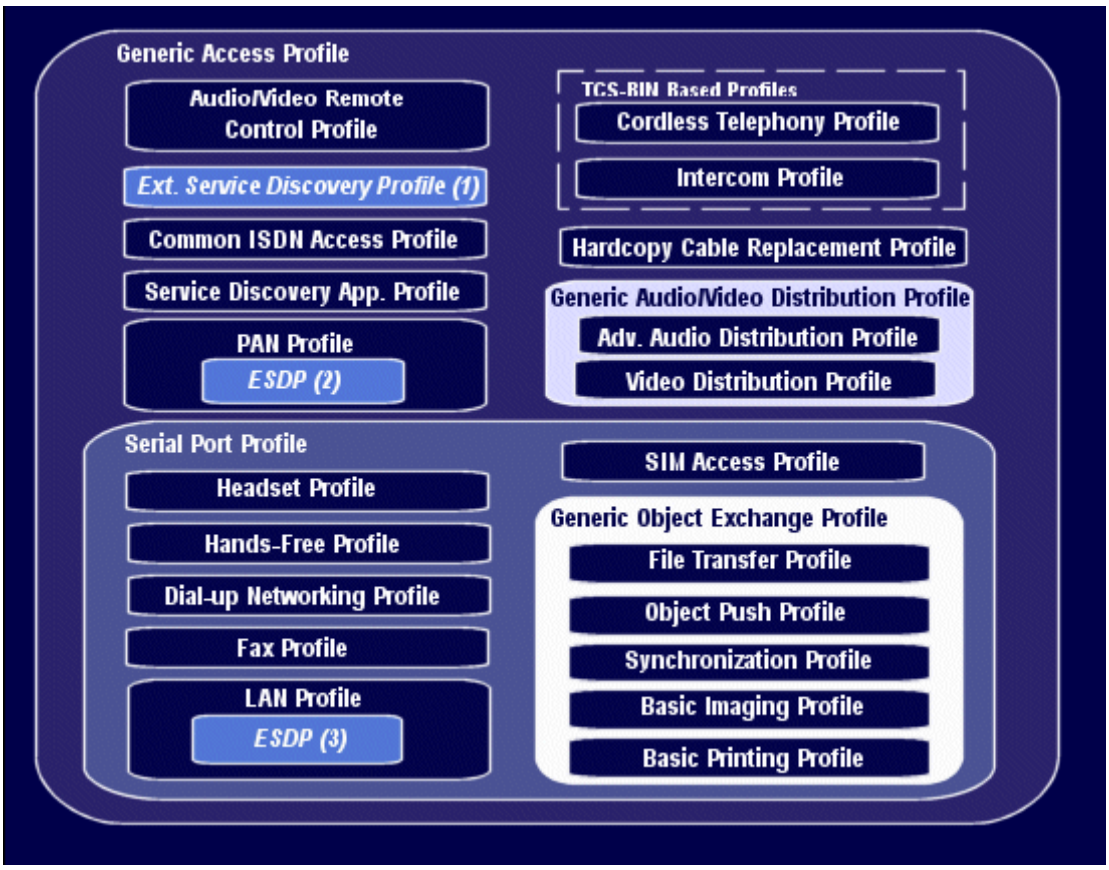
Le concept de profils est utilisé afin d’assurer le maximum de compatibilité entre les produits des différents constructeurs de produits Bluetooth. Ainsi, tous auront les mêmes modèles utilisateurs dans leur couche logicielle : on aura pour tous les appareils Bluetooth les mêmes appellations pour chaque fonctionnalité supportée.

Les profiles Bluetooth ont donc été développés afin de décrire comment implémenter les modèles utilisateur. Ils définissent :

- La manière d'implémenter un usage défini
- Les protocoles spécifiques à utiliser
- Les contraintes et les intervalles de valeurs de ces protocoles

d) Hierarchies des profils

Il existe une hiérarchie entre profil, et donc des dépendances entre eux. Pour illustrer ce phénomène, observons le schéma suivant :



Ainsi, le File Transfert Profil est dépendant du Generic Object Exchange Profile, du Serial
Port Profile, et du Generic Access Profile.

e) Generic Acces Profile

Ce profil est LE profil de base qui doit être implémenté par tous les appareils Bluetooth.
En effet, c'est celui qui définit les procédures génériques de découverte d'équipement, ainsi que de gestion de connexion aux autres appareils Bluetooth.
Pour chaque profil, il existe plusieurs points qui sont redéfinis ou non : rôle, scénario, principes de base…
On utilise les termes d' initiateur et d'Accepteur. Pour les 2 rôles que les protagonistes d'une communication Bluetooth peuvent prendre. L'initiateur est celui qui pour une procédure donnée, est à l'origine de l'établissement d'un lien ou d'une transaction sur un lien existant.
Un utilisateur Bluetooth doit en principe pouvoir se connecter à n'importe quel autre appareil Bluetooth, même si ils n'ont aucune application en commun. Cela doit être possible en utilisant les fonctions basiques de Bluetooth. En effet, il n'y a aucune application commune entre une oreillette Bluetooth Logitech et un téléphone mobile Nokia par exemple.

Ce profil expose l'ensemble des caractéristiques de tous les équipements Bluetooth. Il expose les spécifications sur la représentation des propriétés Bluetooth : l'adresse Bluetooth, le nom d'un équipement, son type, le PIN number utilisé pour authentifier2 périphériques.
Il définit les « modes » génériques à tous les profiles : discoverability mode (on peut le détecter), connectability mode (on peut s'y connecter), pairing mode (on peut créer un lien avec).
Il définit les procédures générales qui peuvent être utilisées pour « découvrir » les propriétés basiques des équipements Bluetooth (nom, type…) qui sont « découvrables».
Il décrit les procédures générales de connexions à d'autres dispositifs Bluetooth et donc la procédure générale de création de liens entre des dispositifs Bluetooth.
Ce profil est celui dont tous les autres dépendent, et tous les profils « héritent » de ses caractéristiques.

f) Autres profils importants

- Service Discovery Application Profile

Ce profil décrit les fonctionnalités et procédures d'une application ou périphérique Bluetooth afin qu'il puisse « découvrir » les services associés à d'autres périphériques Bluetooth et récupérer toute information relative à ces services.
Il définit également les protocoles et procédures à utiliser par une application de détection de services sur un périphérique pour localiser des services disponibles sur d'autres périphériques Bluetooth activés.

- Serial Port Profile

Ce profil est un autre profil principal : en effet, c'est celui qui définit les protocoles et procédures qui doivent être utilisées par les périphériques utilisant Bluetooth pour émuler le protocole RS232 (connexion par câble série, ce que Bluetooth est appelé à remplacer).
De ce profil dépendent les suivants :
- Headset profile : utilisation des casques sans fil ;
- Dial up networking profile : permet d'utiliser un périphérique Bluetooth en tant que pont Internet (possibilité de se connecter à Internet à partir d'un Pocket PC via un téléphone GSM Bluetooth) ;
- Fax profile : envoi/réception de fax via un téléphone GSM Bluetooth
- Etc.…

- Generic Object Exchange Profile

Ce profil définit les spécificités des modèles utilisateur d'échanges d'objets entre périphériques Bluetooth : carte de visite, synchronisation, transfert de fichier…
- File Transfert Profile : utilisé par les applications de transfert de fichier (comme son nom l'indique).
- Synchronisation Profile :Ce profil va permettre à un PDA de synchroniser ses données avec une station de base (ordinateur par exemple via Bluetooth (comme il pourrait le faire via port série, USB ou IrDA).

Il existe d'autres profils Bluetooth permettant de définir d'autres modèles utilisateurs (utilisation d'un récepteur GPS par exemple), et d'assurer la compatibilité de tous les équipements implémentant ces profils entre eux.

IV- Avantages et inconvénients

1- Principal avantage :

- *La liberté du sans fil :*
  Le principal objectif du Bluetooth est bien évidemment une utilisation sans fil, augmentant de manière générale l'ergonomie et l'utilisation des appareils connectés

a) Autre(s) avantage(s) :

- *Pas de contact visuel obligatoire entre les appareils :*
  Grand avantage d'utiliser les ondes radio, les appareils ne sont pas obligatoirement en contact visuel, contrairement à la technologie infrarouge

- *Dérivé de l'USB :*
  Comme cette technologie est une amélioration de l'USB, elle possède aussi les avantages de cette dernière. Les branchements peuvent se faire l'ordinateur allumé et l'installation se fait automatiquement quand le pilote est générique et connu par le système d'exploitation.

- *Le coût :*
  Bluetooth utilise une norme radio qui deviendra un standard international. Son marché potentiel est donc énorme ce qui devrait contribuer à faire chuter les coûts de fabrication des composants. L'utilisateur final ne paiera pas de surcoût sur les appareils équipés de Bluetooth.

- *Et aussi* :
  Faible consommation d'énergie / possibilité d'implantation dans des équipements de petite taille.

2- Principal inconvénient :

- *La sécurité :*
  Première préoccupation des technologies sans fil, la sécurité. En effet, les données circulant par le réseau hertzien, il apparaît théoriquement plus facile de les intercepter que lorsqu'elles circulent dans un câble. Cela pourrait cependant s'avérer être un atout plus tard puisque les trames sont alors plus

cryptées avec les protocoles sans fil. Entre le Bluetooth et Le WIFI, le premier est cependant plus sécurisé puisque la portée est moindre.

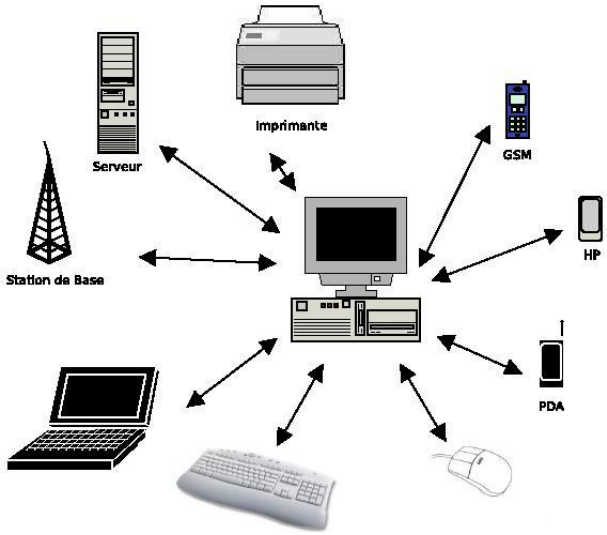
a) Autre(s) inconvénient(s) :

- *Les collisions sur le canal hertzien :*
  La technologie Bluetooth utilise la même fréquence que les ondes radio et que le WIFI (2.4 GHz). Les possibilités de collisions sont donc assez importantes même avec un four à micro-onde par exemple.

- *La portée :*
  Le Bluetooth est moins puissant que le WIFI et sa portée est donc moindre. Elle peut aller jusque 100m mais cette distance diminue suivant le nombre d'obstacles rencontrés.

- *L'utilisation pour les réseaux :*
  Malgré l'existence de réseaux Bluetooth (piconet et scatternet), cette technologie n'est pas adaptée à cet usage, contrairement au WIFI du fait de sa faible portée et de son faible débit.

V- Principaux cas d'utilisation



1- Clavier et souris

Le clavier et la souris peuvent être Bluetooth l'un et l'autre ou les deux en même temps. Des packs sont aujourd'hui disponibles et l'ensemble est relié à l'ordinateur grâce à une clé USB comportant un récepteur Bluetooth.

Le clavier étant l'élément premier où sont saisis mots de passe et codes de cartes bancaires, la technologie Bluetooth utilisant le canal hertzien n'est pas ici la plus recommandée si la sécurité est le premier critère de l'installation.

2- Téléphone portable

La société Ericsson étant l'inventeur du Bluetooth, il n'est pas surprenant que celle-ci s'adresse dans certains cas à l'utilisation des téléphones portables. Notamment concernant les oreillettes, puisque le « sans fil » augmente indéniablement le plaisir d'utilisation. Certaines oreillettes possèdent une autonomie de plus de 2 heures en conversation et de 60 heures en veille. Le protocole Bluetooth a été pensé pour une faible consommation.

3- GPS

Les équipements GPS qui ne sont pas d'origine dans la voiture rattrapent de plus en plus leur retard par rapport à l'installation du constructeur. Le Bluetooth ajoute une nouvelle carte au jeu des équipements GPS non d'origine. Contrairement à certains périphériques comme les claviers et les souris, les pilotes de ces GPS Bluetooth ne sont en général pas génériques et il faudra les installer soi-même.

4- Imprimante

L’impression Bluetooth est surtout avantageuse dans le cas où vous utilisez un appareil photo numérique Bluetooth. L’ordinateur n’est alors plus indispensable pour l’impression des photos.

WIFI

I- Présentation générale

1- A quoi sert le WIFI ?

Le Wi-Fi est une transmission sans fil permettant de relier des ordinateurs portables, des machines de bureau ou tout type de périphérique à une liaison haut débit sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert.

2- WIFI ou 802.11 ?

Un réseau local sans fil n'est pas un réseau WIFI ceci est en fait un abus de langage. Le terme WIFI est une contraction de *Wireless Fidelity* qui correspond au nom donné à la certification délivrée par la WI-FI Alliance. Cet organisme est chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11.
Ainsi un réseau Wifi est en réalité un réseau répondant à la norme 802.11.
La norme *IEEE 802* est un standard international décrivant les caractéristiques d'un réseau local sans fil (*WLAN*)

3- Norme 802.11

La technologie 802.11 a été standardisée à partir de 1997. Au départ, le débit ne dépassait pas 1 à 2 Mbps. Afin d'améliorer les performances des révisions ont été apportées à cette norme.

- **802.11a** : permet un débit théorique de 54 Mbps sur 8 canaux radio dans la bande de fréquence des 5 GHz.

Débit théorique (en intérieur)	Portée
54 Mbits/s	10 m
48 Mbits/s	17 m
36 Mbits/s	25 m
24 Mbits/s	30 m
12 Mbits/s	50 m

- **802.11b** : permet un débit théorique de 11 Mbps sur 13 canaux radio dans la bande de fréquence des 2,4 GHz.

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
11 Mbits/s	50 m	200 m
5,5 Mbits/s	75 m	300 m
2 Mbits/s	100 m	400 m

- **802.11g** : permet un débit 54 Mbps théoriques sur la bande de fréquence des 2.4 GHz. La norme 802.11g à une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peut fonctionner en 802.11b.

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
54 Mbits/s	27 m	75 m
48 Mbits/s	29 m	100 m
36 Mbits/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m

Nom de la norme	Nom	Description
802.11a	Wifi5	La norme 802.11a (baptisé *WiFi 5*) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz.
802.11b	Wifi	La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps rééls) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.
802.11c	Pontage 802.11 vers 802.1d	La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11 (niveau *liaison de données*).
802.11d	Internationalisation	La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.
802.11e	Amélioration de la qualité de service	La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche *liaison de données*. Ainsi cette norme a pour but de définir les besoins des différents paquets en terme de bande passante et de délai de transmission de telle manière à permettre notamment une meilleure transmission de la voix et de la vidéo.
802.11f	Itinérance (roaming)	La norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole *Inter-Access point roaming protocol* permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée *itinérance* (ou *roaming en anglais*)
802.11g		La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b
802.11h		La norme *802.11h* vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, doù le *h* de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.
802.11i		La norme *802.11i* a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'*AES* (*Advanced Encryption Standard*) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.
802.11Ir		La norme *802.11r* a été élaborée de telle manière à utiliser des signaux infra-rouges. Cette norme est désormais dépassée techniquement.
802.11j		La norme *802.11j* est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

II- Équipements

On peut distinguer deux entités dans un réseau sans fil

1- Stations

Les stations équipées d'une carte réseau sans fil (network interface controller ou wirless adaptater) disponibles sous-différents formats (PCI, USB, PCMCIA …).



Les AP points d'accès (Access Point) qui font les liens entre le réseau local câblé et le réseau sans fil.
Les AP donnent accès au réseau filaire auquel il est raccordé aux différentes stations avoisinantes.

2- Points d'accés


Ce sont de concentrateurs pour quelques dizaines de connexions sans fils jusqu'à 11 ou 54 Mbps dans la bande passante de 2,4 GHz, la connexion au réseau filaire se fait via un port 10 base T ou 100 base T.
La portée annoncée est de 90 à 100 m, en réalité à l'intérieur d'un bâtiment en fonction de l'environnement électromagnétique cela fonctionne jusqu'à 30 ou 35 m.

Comme le réseau est un réseau partagé de type hub le débit baisse énormément lorsque le nombre de station et la distance augmentent.
Les AP utilisent le cryptage WEP (wired Equivalent Privacy) sur 40 ou 128 bits pour assurer la confidentialité.
Ils sont administrables par navigateur Web ou système d'administration snmp centralisé.

III- Mise en place d'un radio de type 802.11

La mise en place d'un réseau radio implique une réflexion approfondie autour de l'architecture et de la sécurité.

1- Architecture

En effet, la première chose à faire avant d'installer un réseau WIFI est d'effectuer une étude approfondie de la couverture radio pour cela, il faut essayer de se procurer les plans techniques des bâtiments qui décrivent la structure et les matériaux utilisés, les faux plafonds …
Si cela n'est pas le cas, il faut effectuer un relevé des éléments perturbateurs pour ensuite modéliser l'environnement à l'aide de logiciels de prédiction radio.
Des tests sont ensuite réalisés sur le terrain à l'aide de ces modèles en effectuant des relevés électromagnétiques.
La deuxième chose importante est d'anticiper l'évolution du site, comme le déménagement. Le phénomène est difficile à prévoir pour cela, il peut être partiellement résolu grâce à un mécanisme de gestion automatique de l'émission radio. Les points d'accès ne sont plus complètements autonomes et indépendants mais reliés à un commutateur central qui adapte la puissance de l'émission en fonction des différences observées sur le réseau.
La troisième chose est de déterminer le nombre de bornes à déployer.
Pour pallier, à l'affaiblissement du signal, le constructeur peut proposer une antenne spécifique.
Au lieu d'une émission à 360°, on peut utiliser une antenne directionnelle de 10° par exemple ce qui augmente la porté de l'onde.
Pour éviter les zones d'ombre, il ne faut pas hésiter à superposer les couvertures des différentes bornes.
La quatrième chose est de définir les besoins des utilisateurs, pour anticiper les besoins en bande passante.

La cinquième chose est d'homogénéiser ses protocoles réseaux, en effet si une personne se connecte avec une carte WIFI 802.11b sur un point d'accès 802.11g alors le point d'accès devient 802.11b, ceci limite la bande passante à 11Mbps.
En revanche le mariage entre 802.11a et 802.11g est un plus car il offre une bande passante supplémentaire.

2- Sécurité

Le niveau de sécurité ne sera pas le même si le réseau est considéré comme une extension interne au réseau local ou un WLAN autonome avec accès ou non à Internet par exemple.

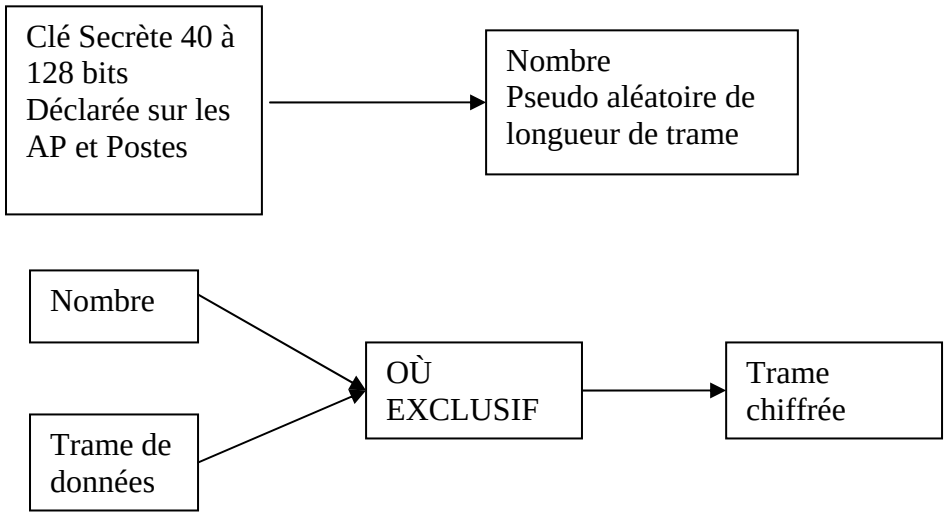
a) Les Risques

- *L'interception de données*

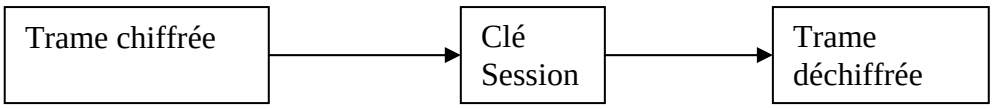
Cela consiste à écouter les transmissions des utilisateurs pour intercepter des données confidentielles pour éviter cela, le standard 802.11 intègre un mécanisme de chiffrement de données, le WEP (Wired Equivalent Privacy).

Principe du WEP :

Chiffrement :



Déchiffrement :



Une attaque par force brute, c'est-à-dire en essayant toutes les combinaisons possibles permet de trouver assez facilement la clé de session.
Il faut donc utiliser au minimum une protection WEP 128 bits ou une autre méthode.
Pour augmenter le niveau de sécurité, on peut coupler le WEP avec une méthode d'authentification.

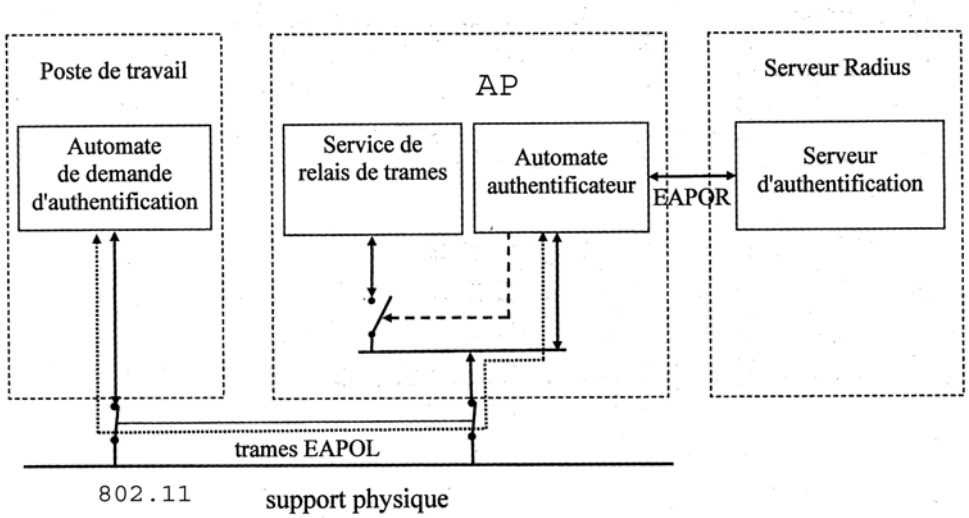
- *Intrusion du réseau*

Principe du 802.1X :

Le standard 802.1X est une solution de sécurisation permettant d'authentifier un utilisateur souhaitant accéder à un réseau grâce à un serveur d'authentification.

Le 802.1X repose sur le protocole EAP (Extensible Authentification Protocol), dont le rôle est de transporter les informations d'identification des utilisateurs.
Principe :
Il faut scinder le port d'accès physique au réseau en 2 ports logiques :

- Un port contrôlé fermé ou ouvert (après authentification) pour les données des utilisateurs.
- Un port non contrôlé toujours ouvert qui ne gère que les trames 801.1X



EAPOL : EAP over LAN
EAPOR : EAP over RADIUS

1. Le contrôleur d'accès PA reçoit une demande de connexion de la part de l'utilisateur, il envoie une requête d'identification auprès du serveur.
2. Le serveur authentification envoie un challenge au contrôleur d'accès, qui le transmet à l'utilisateur. Le challenge est une méthode d'identification, si le client ne gère pas la méthode, le serveur en propose une autre ainsi de suite.
3. L'utilisateur répond au challenge. Si l'identité est correcte, le serveur envoie un accord au contrôleur qui acceptera l'utilisateur sur le réseau.

*Principe du WPA (WIFI Protected Access)**:***

Le WPA est une version allégée du protocole 802.11i, reposant sur des protocoles d'authentification et un algorithme de cryptage : TKI (Temporary Key integrity Prorocol). Ce protocole permet de générer des clés aléatoires et offre la possibilité de modifier la clé de chiffrement plusieurs fois par seconde.
Le fonctionnement de WPA repose sur la mise en œuvre d'un serveur d'authentification.

Pour un petit réseau, on peut utiliser le WPA sans serveur d'authentification.
Il repose sur l'utilisation d'une clé partagée, appelées PSK (pre-shared-key), mais contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur définie, une paraphrase qui est traduite en PSK par un algorithme de hachage.

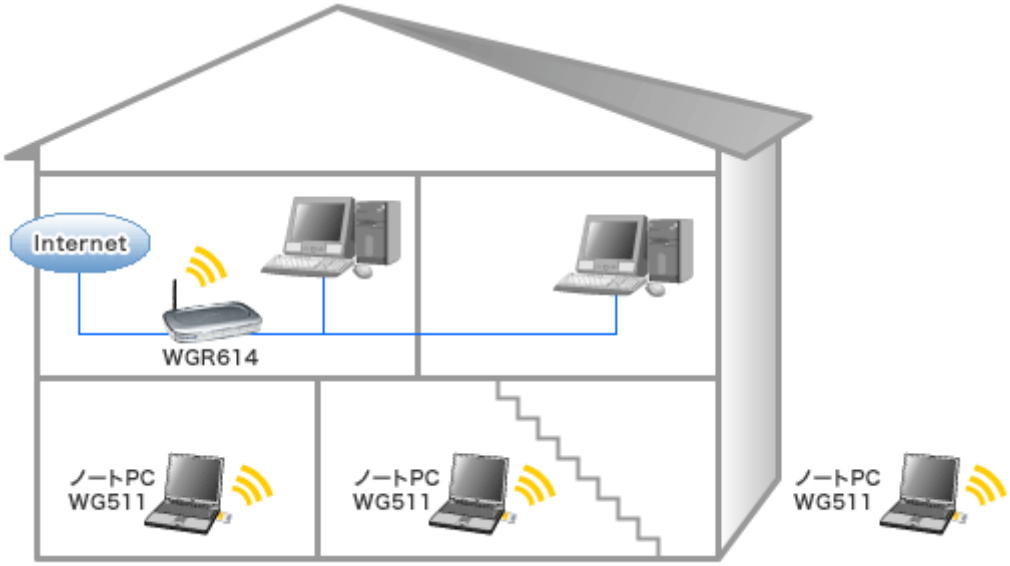
Conclusion : Les méthodes d'authentification évitent l'intrusion du réseau et le chiffrement l'interception de donnée.

Une autre méthode existe qui est plus contraignante sur un réseau important, c'est le filtrage par adresse MAC.
Les AP permettent de gérer une liste de droits d'accès (ACL) basée sur les adresses MAC des équipements autorisés à se connecter.

Dans le cas d'un employé travaillant à distance, on pourra mettre en place un réseau privé virtuel (VPN) crypté SSL ou IPSEC.

Autre problème important, les postes mobiles infectés par les utilisateurs au cours du week-end. Pour cela, on peut séparer le réseau sans fils du reste du réseau en passant par des VLAN.

b) Exemple d'installation



Fonctionnement

Un routeur Wireless Câble/xDSL 54Mbit/s de NETGEAR permet de partager plus facilement une connexion câble/xDSL avec d'autres utilisateurs sur un réseau avec ou sans fils. Le WG614 permet des connexions WAN et LAN 10/100 Mbit/s (auto-

sensing), mais il permet aussi l'interopérabilité avec les appareils des réseaux à 54 Mbit/s (802.11g) et des réseaux à 11 Mbit/s, fonctionnant sur la bande des 2.4GHz.

Sécurité

Un Firewall sécurise le réseau contre les hackers : la fonctionnalité SPI (Stateful Packet Inspection) et la prévention contre les attaques DoS (Denial of Service) préviennent des attaques en scannant le trafic entrant, et la fonction NAT (Network Address Translation) protège les périphériques connectés au réseau des intrus.
Le cryptage WEP (40/64 ou 128 bits) pour les liaisons Wireless du LAN protège les communications des écoutes indiscrètes.
Le contrôle par adresses MAC empêche les accès non autorisé au réseau.
La fonctionnalité VPN pass through permet de sécuriser les liaisons vers une société ou son siège. Une licence gratuite pour 8 PC du logiciel Freedom Zero-Knowledge Systems, qui prévient de l'envoi d'informations personnelles sur Internet, et bloque les publicités.

Sécurité Internet

Le WG614 permet aux parents de limiter l'accès au web en bloquant tout contenu offensif et les URL indésirables. Le routeur envoi des alertes en temps réel et bloque toute connexion avec le web. Une protection anti-virus apporte un surplus de sécurité aux ordinateurs du réseau.

Simplicité

L'assistant rapide simplifie la configuration. Il détecte automatiquement les paramètres et configure le routeur quel que soit l'ISP. L'assistant d'installation, c'est à dire le tutorial interactif de NETGEAR donne des conseils simples pour guider à travers chaque étape de l'installation. Les applications qui supportent l'UpnP (Universal Plug and Play) Le design lisse du WG614 permet l'ajout d'un support vertical pour gagner de l'espace.

Prix

70 euros pour les cartes
150 euros AP /routeur

IV- Mise en place d’un réseau Wi-Fi

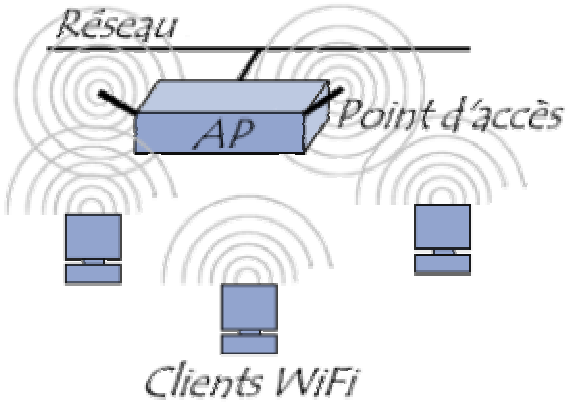
1- Les différentes configurations du réseau

On distingue deux principaux modes :

- **Le mode « infrastructure » :**

On appelle réseau d'infrastructure, un réseau sans fil, dans lequel au moins un point d'accès est présent. Ce point d'accès peut être connecté à un réseau filaire, mais ce n'est pas un impératif.

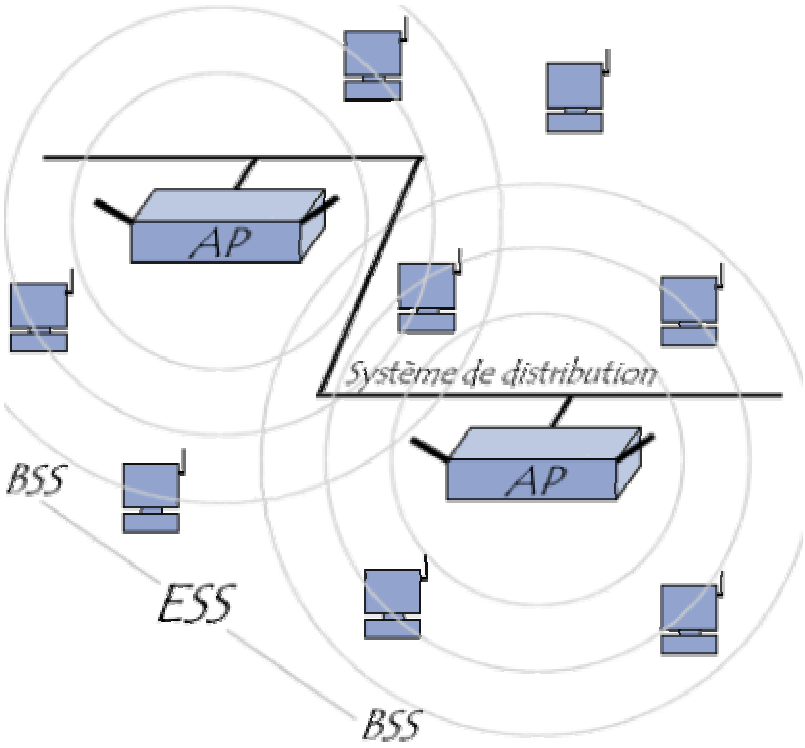
Chaque client sans fil va établir une relation avec le point d'accès qui devient de ce fait le point central du réseau sans fil. L'ensemble des trames transitant sur le réseau sans fil va passer par le point d'accès, même s'il s'agit d'une communication mettant en relation deux stations mobiles connectées au même point d'accès. (similitudes avec la topologie en étoile des réseaux Ethernet)
Dans l'hypothèse où le point d'accès serait lui-même connecté à un réseau local filaire de type Ethernet, il devient la passerelle permettant la connectivité entre les stations sans fil et le reste du réseau telle que le montre le schéma suivant :



Mode Infrastructure

Le point d'accès (noté **AP** pour **A**ccess **P**oint) et l'ensemble des stations (notée **STA**) situées dans la zone de couverture radio de ce dernier constituent une cellule ou **BSS** (**B**asic **S**ervice **S**et).
Chaque BSS est identifié par un **BSSID** (**B**asic **S**ervice **S**et **I**dentifier), un identifiant de 6 octets (48 bits), correspondant à l'adresse MAC du point d'accès.

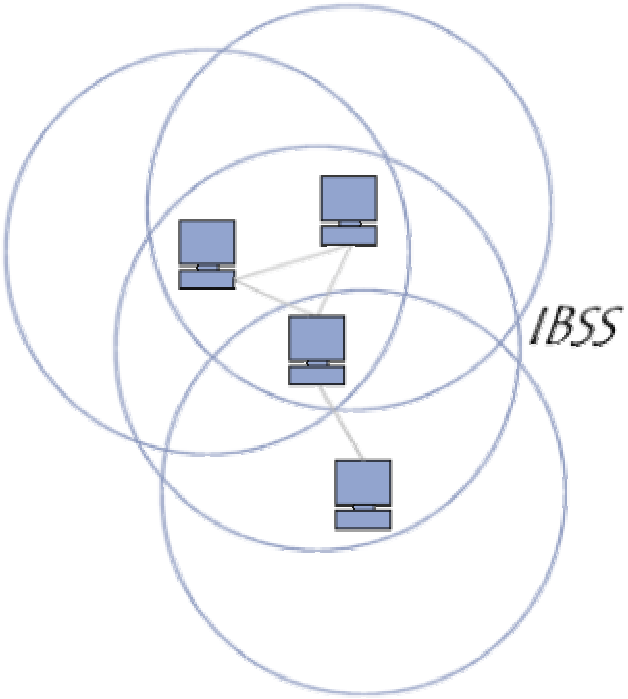
Possibilité d'associer plusieurs BSS formant alors un **ESS** (**E**xtended **S**orted **S**et) grâce à une liaison appelée « système de distribution » (noté **DS** pour Distribution System) comme le montre le schéma suivant :



A la manière du BSS, un ESS dispose d'un **ESSID** (**E**xtended **S**ervice **S**et **I**dentifier) codé sur 32 caractères ASCII pour son identification.
L'ESSID rassemble les adresses MAC des différents points d'accès.

- **Le mode « ad hoc » :**

Dans ce mode, les machines équipées de cartes réseau Wi-Fi se connectent entre elles sans passer par un point d'accès principal.
On parle de réseau « **point à point** » c'est-à-dire un réseau dans lequel chaque machine joue en même temps le rôle de client et le rôle de point d'accès.
Ce mode est approprié à l'échange de fichiers entre 2 ou plusieurs machines.



Mode ad-hoc

L'**IBSS** (**I**ndependant **B**asic **S**ervice **S**et) est le nom du service associé au réseau ad-hoc.

2- Paramètres réseau

a) Le SSID : (Service Set Identifier)

C'est le nom donné au réseau. Il définit le moyen de ralliement des stations entre elles ou des stations avec un point d'accès.
Le SSID est constitué d'un ensemble de 2 à 32 caractères et doit être positionné de manière uniforme, dans l'ensemble des équipements souhaitant échanger des informations au sein du réseau.

Il est important de le personnaliser car souvent il est rentré par défaut dans la borne d'accès par le constructeur.

Le SSID est annoncé par chaque point d'accès de façon régulière dans des trames balise ou beacon. Ainsi, chaque station peut facilement mettre en

place un processus d'écoute du média radio sur chacun des canaux, afin de trouver les réseaux présents dans sa zone.
Une fois un réseau trouvé, il suffit à la station mobile de configurer l'utilisation du même nom de réseau, ou SSID, afin de pouvoir le joindre.
Pour contrer cela, il existe la possibilité de ne pas diffuser le SSID. (option disponible au niveau du paramétrage du routeur faisant office de point d'accès)

b) Canal de transmission des données

Il est nécessaire de spécifier le **canal de transmission** pour chaque station raccordée au point d'accès. (au niveau du routeur)

Le Wi-Fi utilise la technologie **DSSS** (Direct Sequence Spread Spectrum, étalement de spectre à séquence directe) pour la modulation du signal radio. Cette technologie consiste à diviser la porteuse en sous-canaux et fonctionne sur la bande **ISM** (Industrial, Scientific and Medical) des 2,4 GHz.

La bande est divisée en 14 canaux de 20 MHz. La largeur de bande étant de 83,5MHz, les 14 canaux se chevauchent et peuvent générer des pertes de données si 2 canaux se chevauchant sont utilisés dans la même zone d'émission. Une technique appelée « **chipping** » permet de résoudre ces pertes d'informations en effectuant un contrôle d 'erreur.

Il est conseillé de sélectionner des canaux éloignés les uns par rapport aux autres. (stations situées dans la même zone de couverture du point d'accès)

3- A propos des « Hot Spots »

Hot Spot est le raccourci de **Wireless Internet Hotspot** et désigne une aire d'accès Internet haut débit dans un lieu public, utilisant la technologie Wi-Fi.

On les trouve principalement dans les hôtels, les cafés, les aéroports ou les centres commerciaux, dans des espaces ouverts au public mais délimités. (car la zone de couverture radio n'est pas infinie)

Les Hot Spots sont réservés aux utilisateurs informatiques nomades, c'est-à-dire disposant d'un ordinateur portable ou encore d'un assistant personnel (PDA) équipés de la technologie Wi-Fi.

Ils sont en général installés à la demande d'un opérateur spécialisé comme ORANGE, NETOPIA ou du propriétaire du lieu (chaîne hôtelière, association , dirigeant…)

La connexion est soit gratuite (limitée le plus souvent à un intranet d'informations), soit payante en utilisant des cartes pré-payées type Orange Wi-Fi ou un autre type d'abonnement (facturé au temps de connexion par exemple).

De plus en plus, le Hot Spot devient un atout pour attirer le client et procure aux établissements une valeur ajoutée commerciale ou de service.
Certains grands groupes l'ont compris et proposent l'accès gratuit pour leurs clients.

Il y a environ 20000 Hot Spots publics en France. (octobre 2005)

On peut les rechercher sur Internet aux adresses suivantes :

http://www.wifi-world-web.com/fr/
http://wifi.alltelecom.net/

V- Avantages et inconvénients du Wi-Fi

(Concernant l'établissement d'un réseau local d'entreprise ou de particulier)

1- Les avantages

Le premier gros avantage est l'absence de câbles qui permet une flexibilité à toute épreuve sous réserve de posséder quelques notions sur la propagation des ondes radios et être au courant des spécifications de la norme associée. (802.11)
Le réseau Wi-Fi sera alors le complément idéal d'un réseau filaire existant.

Le deuxième avantage, lié fortement au premier, est un coût d'installation très en-deçà de celui d'un réseau filaire qui lui, demande davantage de moyens techniques, logistiques et par conséquent financiers pour sa mise en oeuvre.

Enfin le réseau Wi-Fi reste évolutif : l'ajout d'une station à un point d'accès existant (de préférence un routeur) se fait naturellement et sans encombre à condition de la placer dans la zone d'émission de ce dernier et sans dépasser le nombre limite de stations supportées par ce même point d'accès.
En outre, la fonctionnalité « **roaming** » (itinérance en français) permet de connecter plusieurs points d'accès entre eux (un principal et notion de « répéteur » pour les suivants) donc différents réseaux wi-fi et d'autoriser un utilisateur à passer de l'un à l'autre (en se déplaçant) de manière transparente.

En résumé : FLEXIBLE, BON MARCHE et EVOLUTIF

2- Les inconvénients

Peuvent être liés aux interférences, tout ce qui peut entraver la propagation des ondes radios : four micro-onde et appareils BlueTooth (même fréquence) , l'eau (exemple un aquarium), le corps humain (lorsqu'il y a concentration de personnes essayer de placer en hauteur les antennes), murs épais etc …
Dans ces cas là, le signal n'est pas optimal occasionnant une baisse significative du débit.

En Wi-Fi, la bande passante est partagée c'est-à-dire qu'en cas de connexions simultanées sur le réseau il faudra la diviser par le nombre d'utilisateurs pour obtenir le débit réel sur chacune des machines.

Un réseau mal configuré au niveau sécurité est la porte ouverte au piratage des données y circulant.
Plusieurs techniques existent notamment celle qui consiste à écouter un réseau de l'extérieur d'un bâtiment : les pirates adeptes du « war driving » (concept américain, traduit en France par communauté wi-fi de Montauban) se promènent dans les zones urbanisés et à l'aide d'instruments d'analyse détectent les réseaux Wi-Fi.
Mieux vaut alors sécuriser l'accès du réseau Wi-Fi et essayer de concentrer les ondes émises à l'intérieur du bâtiment (en réglant la puissance d'émission des antennes par exemple).

CONCLUSION

Le WIFI et le Bluetooth se ressemblent sur de nombreux points. Ils utilisent la même technologie, le même canal hertzien mais ont été inventés pour des usages complètement différents. Le Bluetooth a été créé dans le but de corriger les défauts de l'infrarouge et de connecter des périphériques entre eux. Le WIFI a une tout autre finalité. Il ne peut concurrencer le Bluetooth car son encombrement est inadapté à la petite taille des téléphone portable et GPS. De plus sa consommation serait plus importante car les débits plus élevés, donc inadapté à des oreillettes ou souris et clavier sans fil. Une nouvelle norme Bluetooth est cependant en étude concernant le haut débit (802.15.3) et pourrait à l'avenir compliquer les relations entre le Bluetooth et le WIFI.