Introduction aux réseaux sans fil

Pourquoi les réseaux sans fil ?

Relativement récents, les réseaux sans fil sont dorénavant performants grâce notamment aux avancées de l'électronique et du traitement du signal.

Dans les technologies mobiles il y a :
- Les WPAN (Wireless Personal Area Network) : Bluetooth, HomeRF
- Les WLAN (Wireless Local Area Networks) : IEEE 802.11 (US) et Hiperlan (Europe)
- Les technologies cellulaires (GSM, GPRS, UMTS)
- Les technologies Satellite (Vsat qui est bidirectionnel, mais aussi DVB pour la diffusion Vidéo)

Au niveau des opérateurs, le premier réseau commercial analogique sans fil a vu le jour en 1982 à Chicago. En 1986, France Télécom lance Radiocom 2000 en France. Les premiers réseaux GSM (numériques) apparaissent en France en 1992 et remportent le succès que nous connaissons.
Que ce soit au niveau des opérateurs (GSM, GPRS, UMTS), au niveau local (WLAN) ou au niveau domestique (WPAN), de nombreuses applications intéressantes sont envisagées.

Les terminaux s'acheminent vers un support indifférencié de plusieurs protocoles, passant de l'un à l'autre sans rupture de la connexion en fonction de là où on se trouve : GPRS, UMTS, WLAN, BlueTooth. Par exemple lorsque l'on arrive dans un lieu public pour une conférence, on passe sur un WLAN plus rapide que l'UMTS. Autre exemple, actuellement lorsqu'un TGV passe dans d'une cellule GSM à une autre avec tout le monde qui téléphone, les protocoles de changement de cellule se font simultanément pour un grand nombre de personnes. Demain, un WLAN permettra de bénéficier du réseau à l'intérieur du TGV. Le software gérera le choix du protocole à un moment donné : plus de 80% de la R&D dans l'Internet se fait sur le logiciel et non le matériel, selon Gilles Kahn, directeur scientifique de l'INRIA.

Les réseaux sans fil se développent très rapidement et devraient représenter un marché énorme en ce début de XXIème siècle. Les prix jusque là inaccessible deviennent de plus en plus abordables, les performances et les débits augmentent, les réseaux domestiques et la population de travailleurs mobiles également. Le marché des réseaux sans fil est donc en plein essor et certaines analyses estiment ce marché à 2 milliards de dollars pour 2002. Ericsson a avancé le chiffre de 100 millions d'équipements électroniques équipés de la puce Bluetooth en 2002. Les réseaux sans fil représentent donc un enjeu important, surtout au niveau financier : ils permettent d'éviter d'investir dans un câblage coûteux et qui peut s'avérer rapidement obsolète ou inutile en cas de déménagements de locaux.

Nous ne nous intéresserons pas dans ce cours aux réseaux cellulaires dont le but est principalement de transmettre la voix, même si des données peuvent être échangées à faible débit. De même, les réseaux par satellites ne seront pas évoqués. L'accent sera mis sur 3 technologies différentes : la norme 802.11 de l'IEEE, la norme Hiperlan de l'ETSI, et la norme Bluetooth lancée à l'origine par Ericsson qui touche le domaine de la domotique.

Ces différents protocoles ne sont pas compatibles entre eux. Les différents organismes de normalisation et les différents constructeurs tentent chacun d'imposer leur technique. Les débits de transmission vont de 1 à 54 Mbps.

Applications des réseaux sans fil

Les réseaux sans fil peuvent exister en extrémité d'un réseau filaire classique comme Internet et doivent donc pouvoir communiquer avec des machines fixes d'un réseau filaire.

L'intérêt est dans un premier temps de pouvoir assurer une connexion au réseau tout en permettant la mobilité de l'utilisateur. De plus, le câblage n'est plus nécessaire, ce qui représente un avantage certain dans de nombreux cas :
- Mise en place d'un réseau dans un bâtiment classé « monument historique »
- Mise en place d'un réseau de courte durée (chantiers, expositions, locaux loués, formations)
- Confort d'utilisation : tous les participants d'une réunion sont automatiquement interconnectés
- Gain en coût pour la mise en place d'un réseau dans tout bâtiment non préalablement câblé.

De nombreuses autres applications sont envisagées. Dans les hôpitaux, les transmissions sans fil sont déjà utilisées pour accéder aux informations enregistrées sur chaque patient pendant les visites. Des besoins similaires ont été mis en avant par le personnel des aéroports, des chantiers de constructions et autres. Les WLAN peuvent également être utilisés pour la lectures de codes barres dans les supermarchés. Une autre application intéressante est de faire la liaison par voie hertzienne entre deux bâtiments ayant chacun leur réseau câblé.

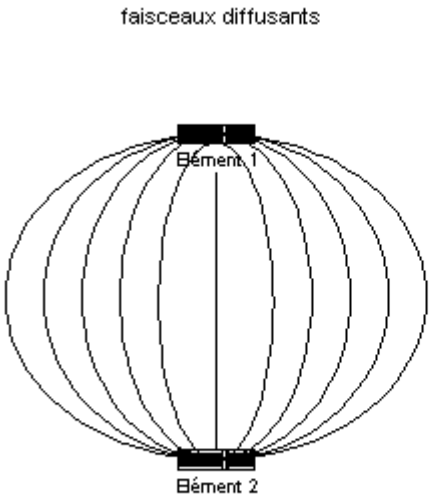
Les WPAN promettent des applications étonnantes qui étaient il y a peu dans le domaine du futurisme. On peut d'ailleurs se demander si l'intérêt des utilisateurs sera en relation avec les fantasmes des industriels…

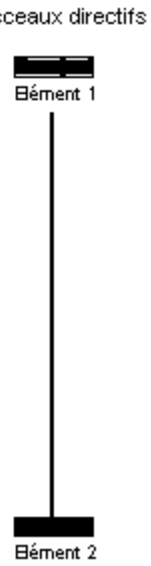
Selon les constructeurs, ces technologies devraient s'étendre dans les prochaines années pour équiper tous les objets de notre vie quotidienne : téléviseurs, chaînes hi-fi, réfrigérateurs, voitures, etc. Les voitures ouvriront leurs portes à la seule approche de leur propriétaire ou communiqueront directement avec la pompe de la station-service, le réfrigérateur fera lui-même sa commande par Internet, les PDA se synchroniseront automatiquement avec les PC et s'échangeront fichiers et e-mails. En arrivant chez vous, la porte d'entrée se déverrouillera automatiquement, le système d'alarme se mettra en veille et les lumières s'allumeront.

Support physique des réseaux sans fil

Plusieurs solutions sont envisagées, la première étant d'avoir une seule borne qui effectue le relais entre les différentes stations par voie hertzienne, la deuxième étant d'avoir des microcellules (typiquement, chaque pièce) qui utilisent l'infrarouge. Les bornes sont dans ce cas interconnectés soit par voie hertzienne, soit par un réseau filaire classique.

Les liaisons infrarouges



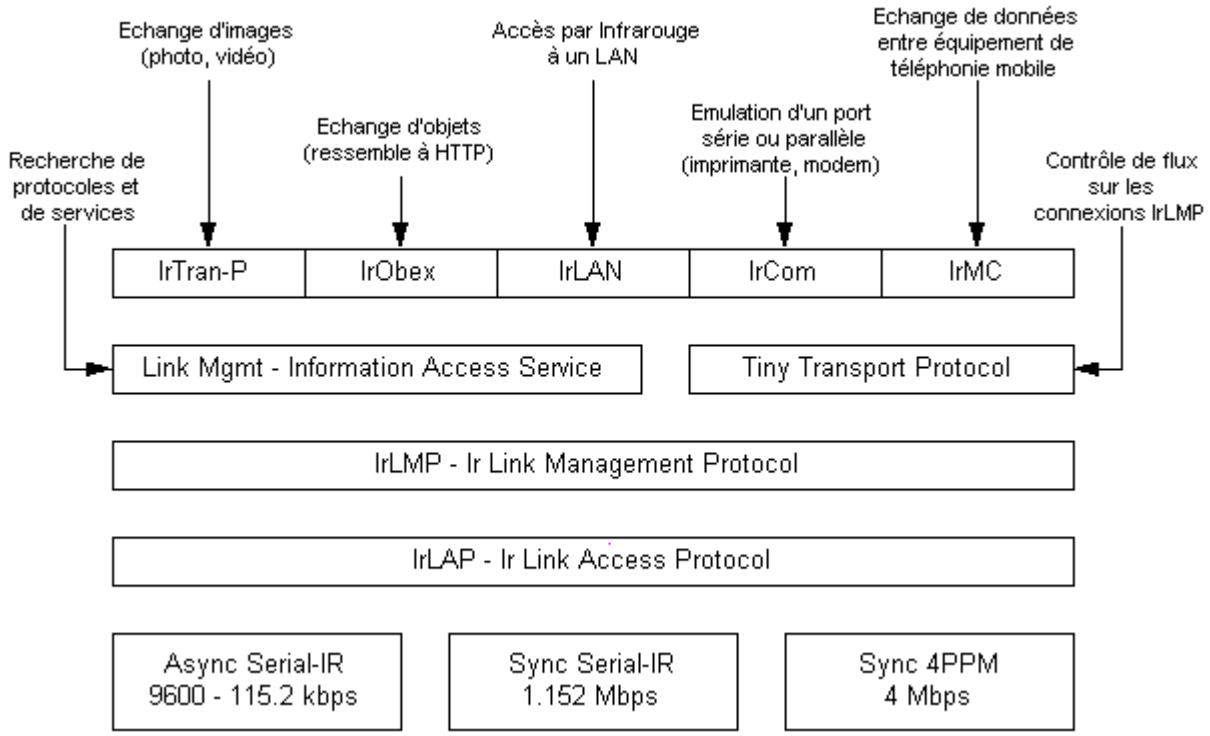


Les liaisons infrarouges sont très utilisées dans le cadre des télécommandes et communications courtes distances où les éléments sont en vue directe, mais sont très sensibles aux perturbations. Si les faisceaux sont directifs, le débit peut être élevé mais rien ne doit passer entre les deux éléments qui communiquent. Les faisceaux diffusants, eux supportent mieux les interférences mais les portées et les débits sont moins élevés.

L'association IrDA (Infrared Data Association), créé en 1994, gère les standards relatifs à la technologie infrarouge. La couche physique (Physical IrDA Sata Signaling) définit typiquement les distances entre éléments à 2 mètres. Des débits de 4 Mbps peuvent être atteints. Des versions courte distance, permettant d'économiser l'énergie, permettent de dialoguer à 30 cm de distance, ce qui est suffisant dans le cas de périphériques de PC.

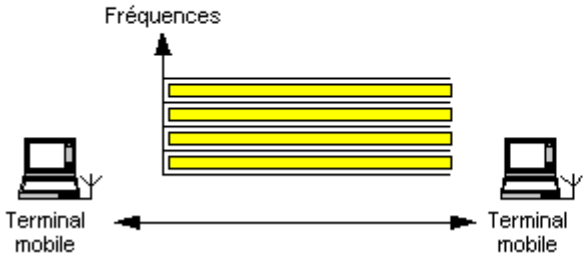
Comme pour tout protocole de communication, le niveau 2 est également défini avec l'IrDA Link Access Protocol (IrLAP) qui gère les connexions entre équipements. L'IrDA Link Management Protocol (IrLMP) gère le multiplexage des informations sur plusieurs canaux et offre un certain nombre de services. Les trames de cette norme ne seront pas étudiées. On y retrouve les champs habituels des protocoles de communication.

Architecture des protocoles IrDA

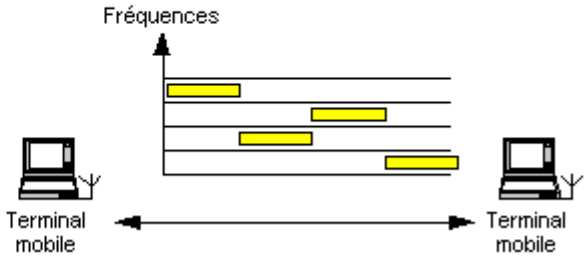


Liaisons radio : Technologies DSSS et FHSS

DSSS : Direct Sequence Spread Spectrum



FHSS : Frequency Hopping Spread Spectrum



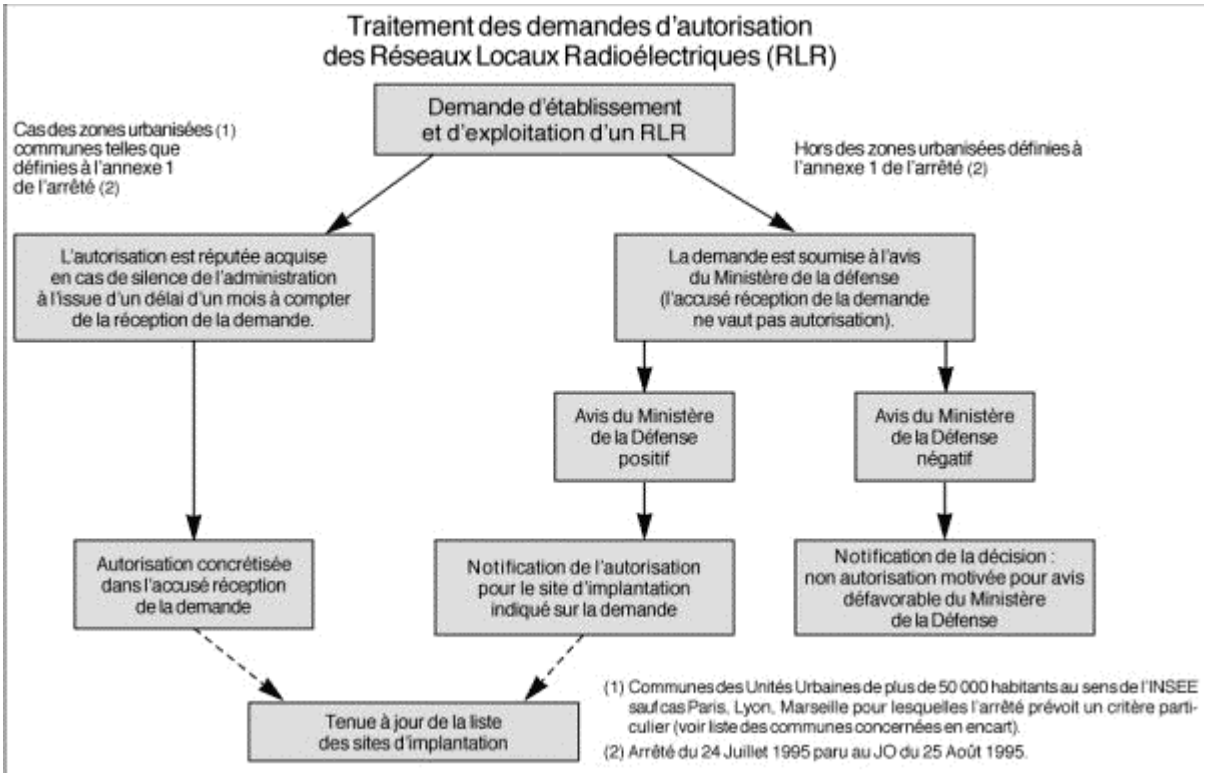
Les réseaux sans fil utilisent les technologies DSSS et FHSS. La technologie DSSS envoie en simultanée l'information sur plusieurs canaux parallèles, ce qui donne un taux d'erreur plus faible (donc un débit plus élevé) et une immunité aux perturbations en bande étroite. La technologie FHSS, elle, est basée sur le saut de fréquence, ce qui permet d'économiser de la bande passante.

Le cadre réglementaire des fréquences en France

Le choix des fréquences utilisées posent un problème de compatibilité entre les différents pays. En effet, selon le pays, ces fréquences peuvent être réservées pour des utilisations militaires ou des services de secours (SAMU, pompiers) qui ne peuvent souffrir d'interférences.

Voici ce que l'on trouve sur le site de l'ART (Autorité de Réglementation des Télécoms) :
Les réseaux locaux radioélectriques (RLR) appelés aussi " RLAN " (pour Radio Local Area Networks) sont constitués d'équipements de transmission de données à large bande permettant différents types d'applications sans fil.
Une norme a été élaborée au niveau européen pour des équipements fonctionnant dans la bande de fréquences 2,4 GHz : l'ETS 300 328. Cette norme d'application volontaire (chaque Etat peut décider ou non de la transposer, pour tout ou partie, dans son droit national) constitue la base d'une recommandation des administrations européennes des postes et télécommunications (CEPT), tendant à harmoniser le régime d'autorisation des équipements concernés afin de favoriser leur développement en Europe.
En France, la bande de fréquences concernée (plus précisément la bande de fréquences 2446,5 MHz - 2483,5 MHz), est utilisée par le Ministère de la défense, qui y a déployé récemment de nouveaux équipements, ce qui ne permet pas d'ouvrir la totalité de la bande de fréquences aux équipements RLR et impose certaines contraintes dues à la coordination avec les Forces Armées.
Les contraintes sont de trois ordres :
- en terme de fréquences : limitation à la bande de fréquences 2446,5 MHz - 2483,5 MHz;
- en terme de formalité administrative : demande individuelle d'établissement (voir formulaire ci-contre);

- en terme d'implantation : les autorisations sont limitées aux communes des unités urbaines de plus de 50 000 habitants et font l'objet d'une procédure simplifiée; dans les autres cas les demandes sont traitées au cas par cas et sont soumises à un accord du Ministère de la défense (il convient pour ces demandes de joindre notamment un plan précisant l'implantation envisagée au sein de la commune concernée).
La procédure de délivrance des autorisations est précisée dans le schéma ci-dessous.



L'étude confiée en 1996 au cabinet de conseil Basic 2000 a dressé un état du marché prospectif des réseaux locaux radioélectriques (RLR) ou " RLAN " en France et en Europe, l'évaluation des perspectives pour Hiperlan (bandes 5 GHz et 17 GHz) et le bilan comparatif de l'environnement réglementaire en Europe.
A ce stade, cette évolution reste toutefois soumise à un accord préalable des forces armées. En revanche s'agissant des réseaux locaux radioélectriques à haute performance (Hiperlan), un régime d'autorisation sans délivrance d'une licence individuelle va être prochainement établi pour l'utilisation d'équipement fonctionnant dans la bande de fréquence 5,15 - 5,25 GHz.

Textes de référence

Arrêté du 24 juillet 1995 relatif aux caractéristiques techniques et d'exploitation des systèmes de transmission de données à large bande utilisant la technologie du spectre étalé dans la bande de fréquences 2.4 GHz (J.O. du 24 Août 1995)

Article 1er - Les systèmes de transmission de données à large bande utilisant la technologie du spectre étalé dans la bande de fréquences 2.4 GHz sont dénommées dans le présent arrêté Réseaux locaux radioélectrique (R.L.R.). Leur établissement et leur exploitation sont autorisés dans la bande de fréquences 2 446.5-2 483.5 MHz dans les conditions définies au présent arrêté, en application de l'article L. 33-2 du codes des postes et télécommunications.

Art. 2 - Les demandes d'autorisation sont adressées à l'administration chargée des télécommunications.
Pour l'implantation de R.L.R. dans les zones urbanisées définies ci-après, l'autorisation est réputée acquise en cas de silence gardé par l'administration à l'issue d'un délai d'un mois à compter de la réception de la demande. Cette autorisation n'est toutefois valable que si les équipements installés sont agréés conformément à la réglementation technique SP/DGPT/ATAS/23.
En dehors des zones urbanisées définies ci-après, l'établissement et l'exploitation des réseaux sont subordonnés à une autorisation expresse de l'administration chargée des télécommunications. L'autorisation n'est délivrée qu'à titre exceptionnel en fonction des résultats d'une étude particulière des contraintes radioélectriques du site d'implantation demandé et après accord du ministère chargé de la défense.

Les zones urbanisées sont constituées des unités urbaines de plus de 50 000 habitants (telles que définies par l'INSEE dans le cadre du recensement général de la population (R.G.P.) de 1990), à l'exception de Paris, Lyon et Marseille pour lesquelles le critère est le suivant :
- pour Paris, est concerné la zone urbanisée définie par l'ensemble des communes inscrites dans un cercle d'un rayon de 30 km autour de Paris ;
- pour Lyon, est concerné la zone urbanisée définie par l'ensemble des communes inscrites dans un cercle d'un rayon de 10 km autour de Lyon ;
- pour Marseille, est concernée la zone urbanisée définie par l'ensemble des communes inscrites dans un cercle d'un rayon de 10 km autour de Marseille, à laquelle s'ajoute la commune d'Aix-en-Provence.

Art. 3 - Les réseaux locaux radioélectriques fonctionnent sans garantie de protection et sur une base de non-interférence avec les équipements

des autres utilisateurs de la bande de fréquences concernée. Le propriétaire ou l'utilisateur d'un R.L.R. est tenu de prendre les mesures nécessaires pour éviter que son réseau ne cause des brouillages aux autres installations radioélectriques régulièrement utilisées.
Ainsi, l'installation des antennes doit être effectuée de telle manière que l'utilisation des réseaux locaux radioélectriques soit limitée au domaine privé concerné.
Art. 4 - Les réseaux locaux radioélectriques ne doivent pas fonctionner avec une puissance isotrope rayonnée équivalente (p.i.r.e.) supérieure à 100 mW.
Pour les systèmes à séquence directe, la limite de densité spectrale de puissance est fixée à - 20 dBW/MHz.

Avantages des réseaux sans fil

Outre la mobilité qui est l'avantage principal de cette technique, le prix peut également être un atout, puisqu'un peu d'électronique peut compenser un câblage manquant. Lors du développement de protocoles de communication sans fil, l'accent est souvent mis sur la configuration et l'installation du matériel : l'installation doit être rapide, simple, et flexible.

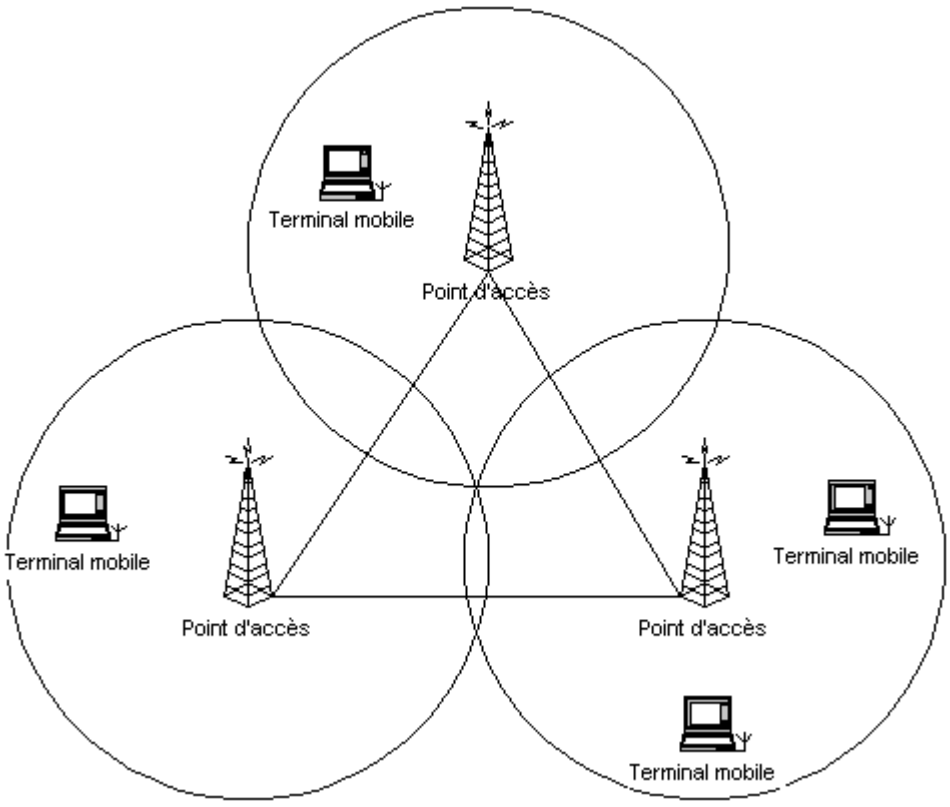
Les évolutions dans les domaines des microprocesseurs, des batteries, permettent aux ordinateurs et téléphones portables et autres PDA (Personal Digital Assistant) de connaître un énorme succès auprès d'un large public. Tous ces terminaux sont appelés à supporter le multimédia et de nouveaux services de télécommunications. Les utilisateurs veulent se déplacer sans s'encombrer d'un câble et avoir accès à toutes les ressources du réseau. Cela demande plus de débit, plus de services, dans des terminaux de plus en plus petits…

Deux modes de fonctionnement

Les WLAN peuvent fonctionner de deux façon différentes : en mode cellule ou en mode ad-hoc.

Le mode infrastructure

Le mode infrastructure fait appel a des bornes de concentration appelées, Points d'Accès, qui gère l'ensemble des communication dans une même zone géographique, comme dans les réseaux GSM. Les bornes sont connectées entre elles par une liaison ou un réseau filaire ou hertzien.



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

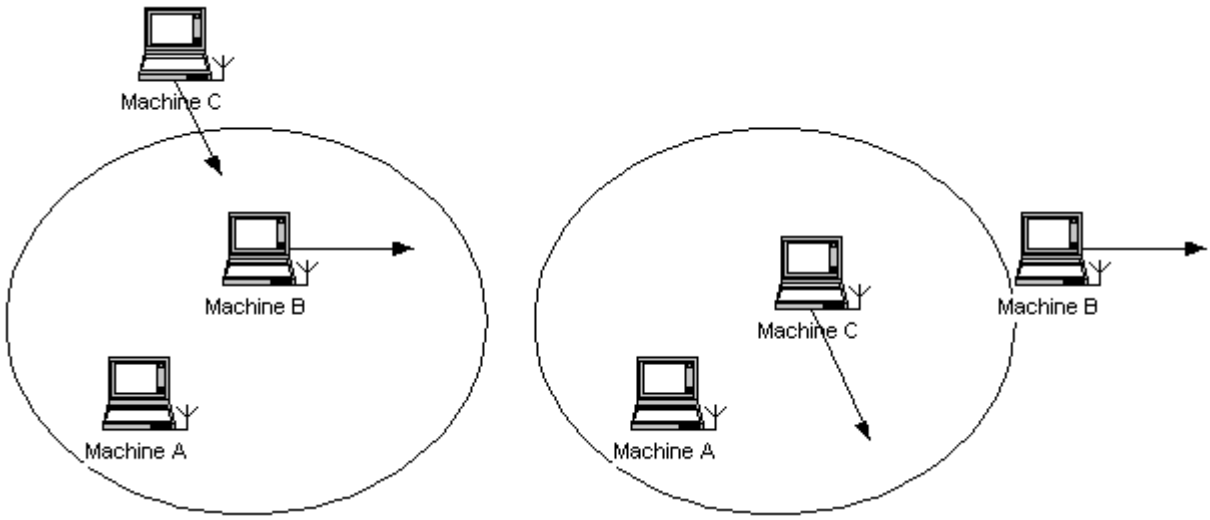
Le mode ad hoc

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.

Les réseaux ad hoc sont un axe de recherche important. Un réseau ad hoc est un réseau sans fil auto-configurable. Lorsque deux machines mobiles ou plus se retrouve dans le même secteur géographique, elles doivent se reconnaître pour pouvoir s'échanger des données. Le réseau doit se configurer automatiquement pour faire la liaison entre ces machines.

Chaque nœud du réseau peut potentiellement échanger des informations avec chaque autre nœud.

Dans le mode de fonctionnement le plus simple, et généralement le seul implémenté dans les protocoles actuels, on considère que les nœuds peuvent échanger des données uniquement lorsqu'elles sont à portée de réception l'une par rapport à l'autre. Dans un mode de fonctionnement idéal, lorsque deux machines ne peuvent se joindre directement, chaque nœud du réseau peut servir de routeur. Les réseaux ad-hoc posent alors implicitement des problèmes de routage entre les machines :



Dans un premier temps, la machine B est dans le rayon de diffusion de la machine A. La machine A et la machine B veulent échanger des informations. La machine B est mobile. Il faut, lorsque la machine B sort du rayon de diffusion de A, que la machine C serve de routeur pour conserver la liaison entre A et B.

Routage dans les réseaux ad hoc

Le routage se fait directement entre les différents mobiles. sans nécessiter un ensemble de bases fixes.

Lorsque l'on veut envoyer des paquets d'un point à un autre, on "inonde" de proche en proche les différents mobiles jusqu'à identifier une route, puis on utilise le chemin ainsi créé pour "router" les données de proche en proche (en fait on définit une route de la destination à la source et on utilise la route inverse)

Un groupe de l'IETF (IP MANET Mobile Ad-hoc NETwork) évalue différents protocoles candidats à la standardisation

- des **protocoles proactifs** (tels que OLSR) où lorsqu'une route est identifiée, elle est stockée dans une table de routage qui est transmise à tous les mobiles, ce qui la rend immédiatement disponible mais génère un important trafic de contrôle

- des **protocoles réactifs** (tels que AODV ou DSR qui permet des liens assymétriques). Dans ce cas on redéfinit les routes à chaque fois. Il n'y a donc plus de trafic de contrôle, mais il y a un coût important en bande passante pour la mise en place des routes et un délai avant chaque ouverture.

- des **protocoles hybrides**, qui utilisent l'une ou l'autre des approches (en dessous d'un certain nombre de saut, l'approche proactive est la meilleure, au dessus, c'est l'approche réactive qui est la plus efficace.

Bluetooth ne peut pas facilement devenir un réseau Ad-Hoc (sans base blueTooth) car il utilise une technique de modulation par saut de fréquence (contrairement aux WLAN qui utilisent l'étalement de spectre) et une base centralisée auxquels se relient tous les appareils plutôt qu'un routage interne

Les avantages et inconvénients du routage radio Ad-Hoc

par rapport au routage classique ou les routeurs sont fixes et reliés par des câbles même si les terminaux sont mobiles.

Avantages : On gagne en mobilité, il n'y a plus d'infrastructure fixe
Inconvénients : On a moins de débit qu'entre des routeurs qui eux sont reliés en général par câble. Les liens ne sont plus isolés les uns des autres (on pollue tout le voisinage à chaque fois contrairement aux liaisons par câbles entre routeur)

La sécurité

Les réseaux sans fil offrent de nouvelles failles aux pirates. De part la nature immatérielle du support physique, l'écoute clandestine sur un réseau sans fil est facile. Il faut donc protéger l'accès aux ressources sans fil et aux informations qui circulent dans les trames.

Les systèmes mobiles sont généralement équipés de processeurs moins puissants que les machines fixes, et ne peuvent se permettre d'effectuer de longs calculs demandés par les systèmes de cryptographie. L'énergie de la batterie est une ressource rare et pose également des problèmes de sécurité.

Les systèmes sans fil sont sensibles à deux attaques principales supplémentaires par rapport aux réseaux classiques. Ces attaques porte atteinte à la disponibilité du réseau et des nœuds :
- Le blocage radio : pour rendre le réseau inutilisable, le pirate peut bloquer les fréquences radio utilisées par le système.
- Epuisement de la batterie : l'attaquant peut interagir avec le nœud dans le seul but de lui faire consommer de la batterie. Les applications doivent donc restreindre leur accès pour éviter ce genre d'attaque.

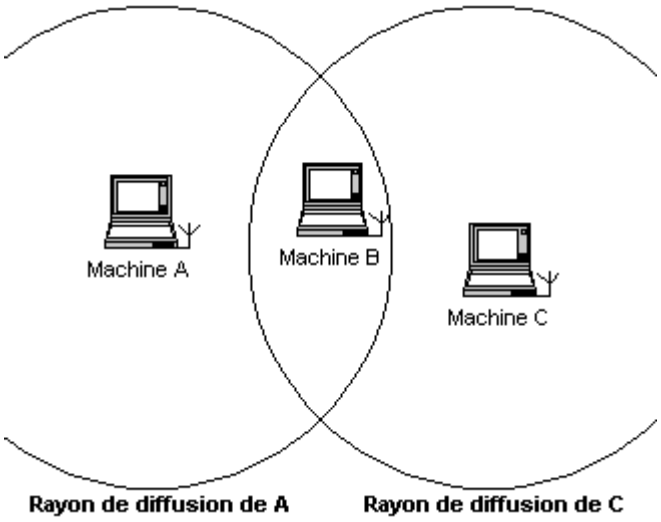
Accès au support physique

Dans les réseaux filaires, les protocoles CSMA sont bien connus, le plus célèbre étant CSMA/CD, utilisé dans Ethernet. Les protocoles CSMA fonctionnent de la façon suivante : Une station voulant émettre écoute le support de transmission, et s'il est occupé (c'est à dire qu'une autre station est en train d'émettre), la station remet sa transmission à plus tard. Si le support est libre, la station est autorisée à transmettre.

Ce type de protocole est très efficace lorsque le support n'est pas surchargé, mais il existe toujours une chance pour que 2 stations émettent en même temps et créent ainsi une collision. Ainsi, le but revient à détecter ces collisions pour que la couche MAC puisse retransmettre la trame sans avoir à repasser par les couches supérieures, ce qui engendrerait des délais significatifs. Dans Ethernet, la détection des collisions se fait par l'écoute du support lorsque la station transmet.

Ce type de fonctionnement n'est pas possible dans un environnement sans fils pour 2 raisons :
- Implémenter un mécanisme de détection de collision demanderait l'implémentation d'une liaison radio full duplex.
- Toutes les stations ne s'entendent pas forcement entre elles car chaque station à une portée d'écoute limitée, et le fait que la station voulant transmettre teste si le support est libre, ne veut pas forcément dire que le support est libre autour du récepteur.

Ainsi, le problème revient à savoir s'il existe des interférences dans la zone du récepteur. C'est le problème de la « station cachée ».



Exemple : La station A veut transmettre des données à la station B.
Si la station C écoute le support, elle n'entend pas A car il est hors de portée de C : elle peut conclure faussement qu'aucune transmission n'est en cours dans son entourage. Si C commence à transmettre, des interférences avec les trames de A auront lieu dans l'entourage de B.

Introduction

Le but de ce document est de donner un aperçu technique du standard 802.11, de façon à comprendre les concepts de base, le principe des opérations, et quelques raisons expliquant telle fonction ou tel composant du standard.

De toute évidence, ce document ne couvre pas l'ensemble du standard et ne donne pas assez d'informations pour implémenter un élément compatible 802.11. Pour cela, il est préférable de lire directement le standard qui comporte plusieurs centaines de pages.

Cette version (juillet 1997) s'occupe principalement des aspects fonctionnels et MAC. Cette norme a évolué, notamment vers des débits plus importants (11 Mbps)

Architecture IEEE 802.11

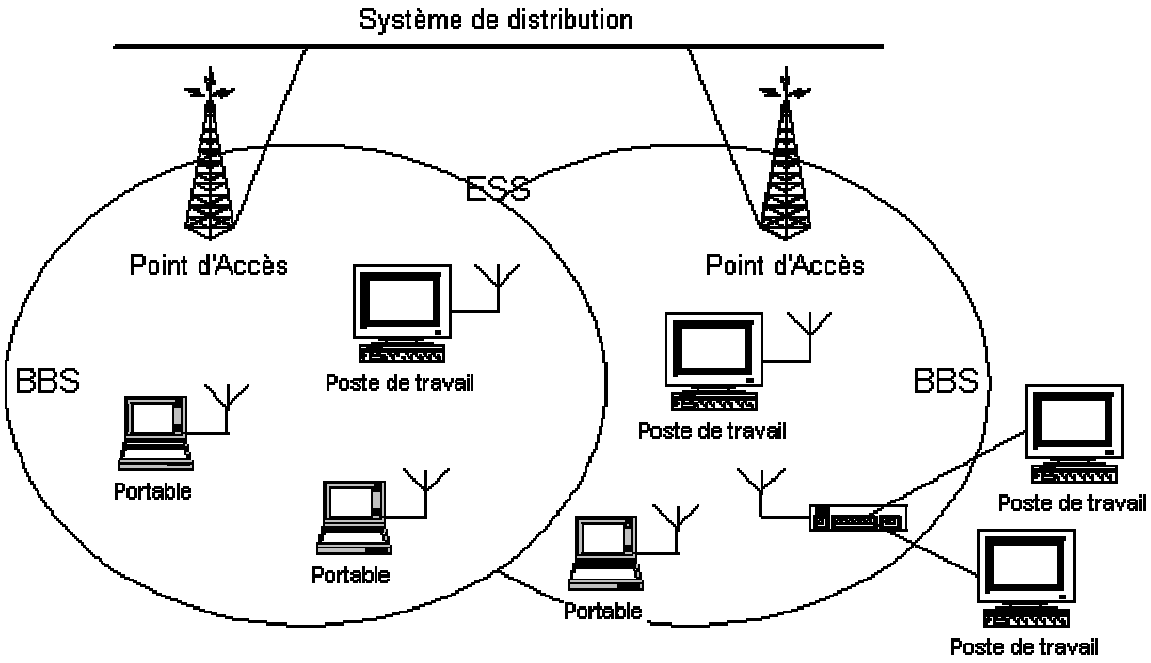
Les composants de l'architecture

Un réseau local 802.11 est basé 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).

Même si un réseau local sans fil peut être formé par une cellule unique, avec un seul Point d'Accès, (et comme décrit plus loin, il peut même fonctionner sans Point d'Accès), la plupart des installations seront formées de plusieurs cellules, où les Points d'Accès sont interconnectés par une sorte de backbone (appelé Distribution System ou DS, Système de Distribution en français), typiquement Ethernet, et dans certains cas, lui-même sans fil.

L'ensemble du réseau local sans fil interconnecté, incluant les différentes cellules, leurs Points d'Accès respectifs et le Système de Distribution, est vu par les couches supérieures du modèle OSI comme un unique réseau 802, et est appelé dans le standard Extented Service Set (ESS).

Le schéma suivante montre un LAN 802.11 typique, avec les composants décrits précédemment :



Le standard définit également le concept de « Portail », un Portail est un élément qui s'interconnecte entre un réseau local 802.11 et un réseau local 802. Ce concept est une description abstraite d'une partie de fonctionnalité d'un pont de translation (translation bridge).

Même si le standard ne le demande pas nécessairement, les installations typiques auront le Point d'Accès et le Portail sur une même entité.

Description des couches IEEE 802.11

Comme tout 802.x, le protocole 802.11 couvre les couches MAC et physique. Le standard définit actuellement une seule couche MAC qui interagit avec trois couches physiques, fonctionnant toutes les trois à 1 et 2 Mbps :

- Frequency Hopping Spread Spectrum dans la bande des 2,4 GHz
- Direct Sequence Spread Spectrum dans la bande des 2,4 GHz
- Infrarouge

<table>
<tr><td colspan="3">802.2</td><td rowspan="2">Liaison de données</td></tr>
<tr><td colspan="3">802.11</td></tr>
<tr><td>FH</td><td>DS</td><td>IR</td><td>Physique</td></tr>
</table>

En plus des fonctions habituellement rendues par la couche MAC, la couche MAC 802.11 offre d'autres fonctions qui sont normalement confiées aux protocoles supérieurs, comme la fragmentation, les retransmissions de paquet et les accusés de réception.

La couche MAC définit deux méthodes d'accès différentes, la Distributed Coordination Function et la Point Coordination Function.

La méthode d'accès de base : CSMA/CA

Le mécanisme d'accès de base, appelé Distributed Coordination Function est typiquement le mécanisme Carrier Multiple Acces with Collision Avoidance (CSMA/CA). Les protocoles CSMA sont bien connus de l'industrie, où le plus célèbre est Ethernet, qui est un protocole CSMA/CD (CD pour Collision Detection).

Un protocole CSMA fonctionne comme suit : une station voulant émettre écoute le support de transmission, et si le support est occupé (ie. une autre station est en train d'émettre), alors la station remet sa transmission à plus tard. Si le support est libre, la station est autorisée à transmettre.

Ces types de protocoles sont très efficaces quand le support n'est pas surchargé, puisqu'il autorise les stations à émettre avec un minimum de délai, mais il y a toujours une chance que des stations émettent en même temps (collision). Ceci est dû au fait que les stations écoutent le support, le repèrent libre, et finalement décident de transmettre, parfois en même temps qu'une autre exécutant cette même suite d'opérations.

Ces collisions doivent être détectées, pour que la couche MAC puisse retransmettre le paquet sans avoir à repasser par les couches supérieures, ce qui engendrerait des délais significatifs. Dans le cas d'Ethernet, cette collision est repérée par les stations qui transmettent, celles-ci allant à la phase de

retransmission basée sur un algorithme de retour aléatoire exponentiel (exponential random backoff).

Si ces mécanismes de détection de collision sont bons sur un réseau local câblé, ils ne peuvent pas être utilisés dans un environnement sans fil, pour deux raisons principales :
1. Implémenter un mécanisme de détection de collision demanderait l'implémentation d'une liaison radio full duplex, capable de transmettre et de recevoir immédiatement, une approche qui en augmenterait significativement le prix.
2. Dans un environnement sans fil, on ne peut être sûr que toutes les stations s'entendent entre elles (ce qui est l'hypothèse de base du principe de détection de collision), et le fait que la station voulant transmettre teste si le support est libre, ne veut pas forcement dire que le support est libre autour du récepteur.

Pour combler ces problèmes, 802.11 utilise le mécanisme d'esquive de collision (Collision Avoidance), ainsi que le principe d'accusé de réception (Positif Acknowledge), comme suit :
Une station voulant transmettre écoute le support, et s'il est occupé, la transmission est différée. Si le support est libre pour un temps spécifique (appelé DIFS, Distributed Inter Frame Space, dans le standard), alors la station est autorisée à transmettre. La station réceptrice va vérifier le CRC du paquet reçu et renvoie un accusé de réception (ACK). La réception de l'ACK indiquera à l'émetteur qu'aucune collision n'a eu lieu. Si l'émetteur ne reçoit pas l'accusé de réception, alors il retransmet le fragment jusqu'à ce qu'il l'obtienne ou abandonne au bout d'un certain nombre de retransmissions.

Virtual carrier Sense

Pour réduire la probabilité d'avoir deux stations entrant en collision car ne pouvant pas s'entendre l'une l'autre, le standard définit le mécanisme de Virtual Carrier Sense (sensation virtuelle de porteuse) :

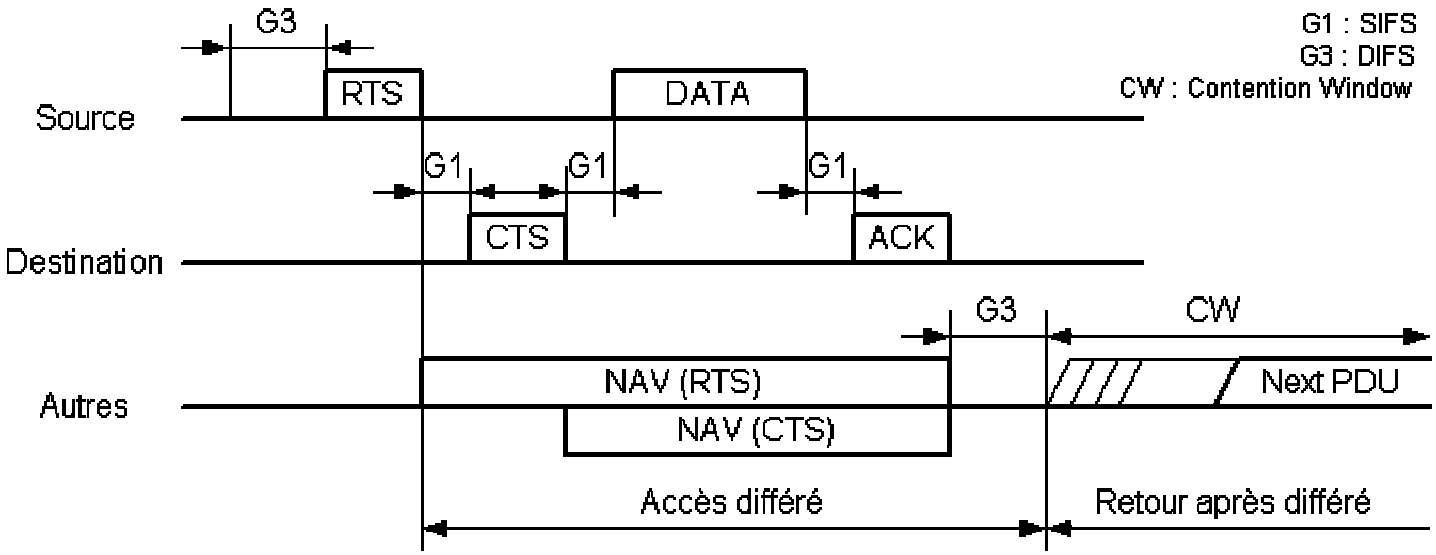
Une station voulant émettre transmet d'abord un petit paquet de contrôle appelé RTS (Request To Send), qui donnera la source, la destination, et la durée de la transaction (ie. le paquet et son accusé de reception). La station destination répond (si le support est libre) avec un paquet de contrôle de réponse appelé CTS (Clear To Send), qui incluera les mêmes informations sur la durée.

Toutes les stations recevant soit le RTS, soit le CTS, déclencheront leur indicateur de Virtual Carrier Sense (appelé NAV pour Network Allocation Vector), pour une certaine durée, et utiliseront cette information avec le Physical Carrier Sense pour écouter le support.

Ce mécanisme réduit la probabilité de collision par une station « cachée » de l'émetteur dans la zone du récepteur à la courte durée de transmission du RTS, parce que la station entendra le CTS et considèrera le support comme occupé jusqu'à la fin de la transaction. L'information « durée » dans le RTS protège la zone de l'émetteur des collisions pendant la transmission de l'accusé de réception (par les stations étant hors de portée de la station accusant réception).

Il est également à noter que grâce au fait que le RTS et le CTS sont des trames courtes, le nombre de collisions est réduit, puisque ces trames sont reconnues plus rapidement que si tout le paquet devait être transmis (ceci est vrai si le paquet est beaucoup plus important que le RTS, donc le standard autorise les paquets courts à être transmis sans l'échange de RTS/CTS, ceci étant contrôlé pour chaque station grâce au paramètre appelé RTSThreshold).

Le diagramme suivant montre une transaction entre deux stations A et B, et la valeur du NAV de leurs voisins :



L'état NAV est combiné au Physical Carrier Sense pour indiquer l'état occupé du support.

Accusés de réception du niveau MAC

Comme mentionné précédemment dans ce document, la couche MAC s'occupe de la détection de collision par l'attente d'un accusé de réception (ACK)

pour chaque fragment transmis (la seule exception à ça étant les paquets qui ont plus d'une destination, comme le multicast, qui n'ont pas de réponse ACK).

Fragmentation et réassemblage

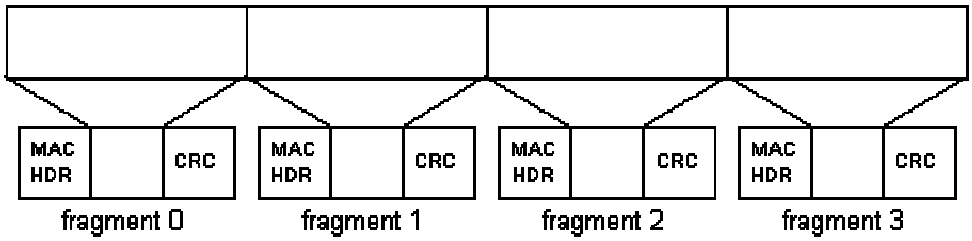
Les protocoles de réseaux locaux classiques utilisent des paquets de plusieurs centaines d'octets (eg. les paquets Ethernet peuvent atteindre 1518 octets). Dans un environnement de réseau local sans fil, il y a des plusieurs raisons d'utiliser des paquets plus petits :
- A cause du taux d'erreur par bit qui est plus important sur une liaison radio. La probabilité d'un paquet d'être corrompu augmente avec sa taille.
- Dans le cas d'un paquet corrompu (à cause d'une collision ou même du bruit), plus le paquet est petit, moins le surdébit engendré par sa retransmission est important.
- Dans un système à saut de fréquence, le support est interrompu périodiquement pour ce changement de fréquence (dans notre cas, toutes les 20 ms), donc plus le paquet est petit, plus la chance d'avoir une transmission interrompue est faible.

D'un autre côté, il n'est pas utile de créer un nouveau protocole LAN incapable de traiter les paquets de 1518 octets utilisés sur Ethernet. Le comité a donc décidé de résoudre ce problème en ajoutant un simple mécanisme de fragmentation et réassemblage au niveau de la couche MAC.

Ce mécanisme se résume à un algorithme simple d'envoi et d'attente de résultat, où la station émettrice n'est pas autorisée à transmettre un nouveau fragment tant qu'un des deux évènements suivants n'est pas survenu :
1. Réception d'un ACK pour ledit fragment.
2. Décision que le fragment a été retransmis trop souvent et abandon de la transmission de la trame.

Il est à noter que le standard autorise la station à transmettre à une adresse différente entre les retransmissions d'un certain fragment. Ceci est particulièrement utile quand un Point d'Accès a plusieurs paquets en suspens pour plusieurs destinations différentes et qu'une d'entre elles ne répond pas.

Le diagramme suivant montre une trame (MSDU) qui a été divisée en plusieurs fragments (MPDUs) :



Inter Frame Space (espace entre deux trames)

Le standard définit 4 types d'espace en entre deux trames, utilisés pour leurs différentes propriétés :

- SIFS (Short Inter Frame Space) est utilisé pour séparer les transmissions appartenant à un même dialogue (eg. Fragment – Ack). C'est le plus petit écart entre deux trames et il y a toujours, au plus, une seule station pour transmettre à cet instant, ayant donc la priorité sur toutes les autres stations. Cette valeur est fixée par la couche physique et est calculée de telle façon que la station émettrice sera capable de commuter en mode réception pour pouvoir décoder le paquet entrant. Pour la couche physique FH de 802.11, cette valeur est de 28 microsecondes.
- PIFS (Point Coordination IFS) est utilisé par le Point d'Accès (appelé point coordinateur dans ce cas) pour gagner l'accès au support avant n'importe quelle autre station. Cette valeur est SIFS plus un certain temps (Slot Time, défini dans le paragraphe suivant), soit 78 microsecondes.
- DIFS (Distributed IFS) est l'IFS utilisé par une station voulant commencer une nouvelle transmission, et est calculé comme étant PIFS plus un temps, soit 128 microsecondes.
- EIFS (Extended IFS) est l'IFS le plus long. Il est utilisé par une station recevant un paquet qu'elle ne comprend pas. Ceci est nécessaire pour éviter que la station (celle qui ne comprend pas l'information de durée pour le Virtual Carrier Sense) ne provoque de collision avec un futur paquet du dialogue en cours.

Algorithme de backoff exponentiel

Le backoff est une méthode bien connue pour résoudre les différents entre plusieurs stations voulant avoir accès au support. Cette méthode demande que chaque station choisisse un nombre aléatoire n entre 0 et un certain nombre, et d'attendre ce nombre de slots avant d'accéder au support, toujours en vérifiant qu'une autre station n'a pas accédé au support avant elle.

Le durée d'un slot (Slot Time) est défini de telle sorte que la station sera toujours capable de déterminer si une autre station a accédé au support au début du slot précédent. Cela divise la probabilité de collision par deux.

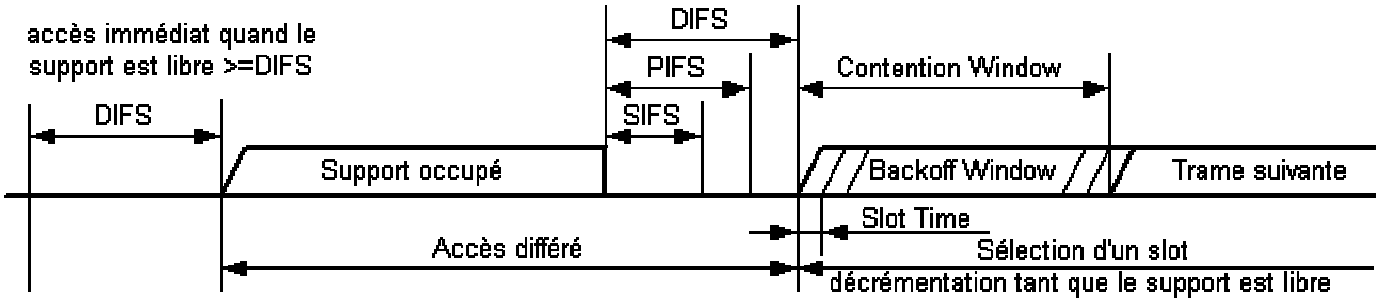
Le backoff exponentiel signifie qu'à chaque fois qu'une station choisit un slot et provoque une collision, le nombre maximum pour la sélection aléatoire est augmenté exponentiellement.

Le standard 802.11définit l'algorithme de backoff exponentiel comme devant être exécuté dans les cas suivant :
- Quand la station écoute le support avant la première transmission d'un paquet et que le support est occupé.
- Après chaque retransmission

- Après une transmission réussie

Le seul cas où ce mécanisme n'est pas utilisé est quand la station décide de transmettre un nouveau paquet et que le support a été libre pour un temps supérieur au DIFS.

La figure suivante montre le principe du mécanisme d'accès :



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 cellule), la station a besoin d'informations de synchronisation de la part du Point d'Accès (ou des autres stations pour le mode ad hoc que l'on verra plus tard).

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

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.

Le roaming

Le roaming est le processus de mouvement d'une cellule vers une autre sans fermer la connexion. Cette fonction est similaire au « handover » des téléphones portables, avec deux différences majeures :
- Sur un LAN, qui est basé sur des paquets, la transition d'une cellule à une autre doit être faite 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 dans les LAN, mais…
- Dans un système vocal, une déconnexion temporaire peut ne pas affecter la conversation, alors que dans un environnement de paquets, 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. Celles-ci comprennent 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.

Rester synchronisé

Les stations doivent rester synchronisées. Ceci est nécessaire pour garder la synchronisation au cours des sauts, ou pour d'autres fonctions comme l'économie d'énergie. Sur une mêmecellule, ceci est obtenue car toutes les stations synchronisent leur horloge avec l'horloge du Point d'Accès en utilisant le mécanisme suivant :

Le Point d'Accès transmet périodiquement des trames appelées « trames balise ». Ces trames contiennent la valeur de l'horloge du Point d'accès au

moment de la transmission (notons que c'est le moment où la transmission à réellement lieu, et non quand la transmission est mise à la suite des transmissions à faire. Puisque la trame balise est transmise selon les règles du CSMA, la transmission pourrait être différée significativement).

Les stations réceptrices vérifient la valeur de leur horloge au moment de la réception, et la corrige pour rester synchronisées avec l'horloge du Point d'Accès. Ceci évite des dérives d'horloge qui pourraient causer la perte de la synchronisation au bout de quelques heures de fonctionnement.

Sécurité

La sécurité est le premier 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 en utilisant le même équipement sans fil
- Capturer le trafic du réseau sans fil (écoute clandestine)

Prévenir l'accès aux ressources du réseau

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.

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. Le générateur de nombres pseudo aléatoires ressort une séquence de clefs de bits pseudo aléatoires, égales en longueur au paquet le plus large possible, qui, combiné avec des paquets entrants ou sortants produit le paquet transmis par la voie des airs.

L'algorithme WEP est un simple algorithme basé sur l'algorithme RC4 de RSA, qui a les propriétés suivantes :
- Raisonnablement fort : l'attaque par force brute de cet algorithme est difficile par le fait que chaque trame est envoyée avec un vecteur d'initialisation qui relance le générateur de nombres pseudo aléatoires.
- Autosynchronisation : l'algorithme se resynchronise pour chaque message. Ceci est nécessaire pour travailler en mode non connecté, où les paquets peuvent être perdus, comme dans tout réseau local.

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, derrière le mécanisme d'économie d'énergie, 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.

Les Points d'Accès transmettent aussi périodiquement (dans les trames balise) des informations spécifiant quelles stations ont des trames stockées par le Point d'Accès. Ces stations peuvent ainsi se réveiller pour récupérer ces trames balise, et si elles contiennent une indication sur une trame stockée en attente, la station peut rester éveillée pour demander à récupérer ces trames.

Les trames de multicast et de broadcast sont stockées par le Point d'Accès et transmises à certains moments (chaque DTIM) où toutes les stations en mode d'économie d'énergie qui veulent recevoir ce genre de trames devraient rester éveillées.

Types de trame

Il y a trois principaux types de trames :
- Les trames de données, utilisées pour la transmission des données
- Les trames de contrôle, utilisées pour contrôler l'accès au support (eg. RTS, CTS, ACK)
- Les trames de gestion, transmises de la même façon que les trames de données pour l'échange d'informations de gestion, mais qui ne sont pas transmises aux couches supérieures.

Chacun de ces trois types est subdivisé en différents sous-types, selon leurs fonctions spécifiques.

Format des trames

Toutes les trames 802.11 sont composées des composants suivants :

Préambule

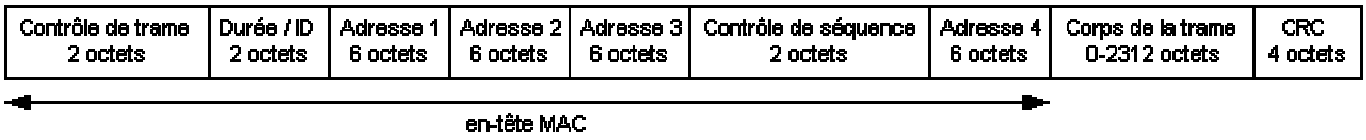
Il est dépendant de la couche physique et comprend :
- Synch : c'est une séquence de 80 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne appropriée (si plusieurs sont utilisées), et pour corriger l'offset de fréquence et de synchronisation.
- SFD : Le Start Frame Delimiter consiste en la suite de 16 bits 0000 1100 1011 1101, utilisée pour définir le début de la trame.

En-tête PCLP

L'en-tête PCLP est toujours transmis à 1 Mbps et contient des informations logiques utilisées par la couche physique pour décoder la trame :
- Longueur de mot du PLCP_PDU : il représente le nombre d'octets que contient le paquet, ce qui est utile à la couche physique pour détecter correctement la fin du paquet.
- Fanion de signalisation PLCP : il contient seulement l'information de taux, encodé à 0,5 Mbps, incrémenté de 1 Mbps à 4,5 Mbps
- Champ d'en-tête du contrôle d'erreur : champ de détection d'erreur CRC 16 bits.

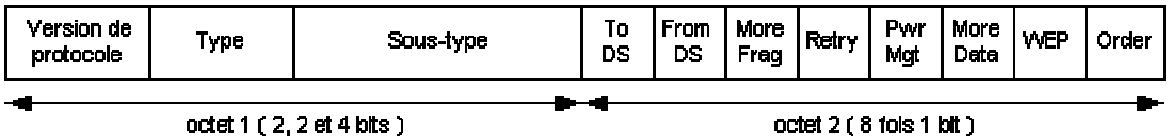
Données MAC

La figure suivante montre le format général de la trame MAC, certains champs sont seulement présents dans une partie des trames, comme décrit ultérieurement.



Contrôle de trame

le champ de contrôle de trame contient les informations suivantes :



- **Version de protocole** : ce champ contient 2 bits qui pourront être utilisés pour reconnaître des versions futures possibles du standard 802.11. Dans la version courante, la valeur est fixée à 0.

- **Type et sous-type** : les 6 bits définissent le type et le sous-type des trames :

Valeur du type (b3 b2)	Description du type	Valeur du sous-type (b7 b6 b5 b4)	Description du sous-type
00	Gestion	0000	Requête d'association
00	Gestion	0001	Réponse d'association
00	Gestion	0010	Requête de ré-association
00	Gestion	0011	Réponse de ré-association
00	Gestion	0100	Demande d'enquête
00	Gestion	0101	Réponse d'enquête
00	Gestion	0110-0111	Réservés
00	Gestion	1000	Balise
00	Gestion	1001	ATIM
00	Gestion	1010	Désassociation
00	Gestion	1011	Authentification
00	Gestion	1100	Désauthentification
00	Gestion	1101-1111	Réservés
01	Contrôle	0000-1001	Réservés
01	Contrôle	1010	PS-Poll
01	Contrôle	1011	RTS
01	Contrôle	1100	CTS
01	Contrôle	1101	ACK
01	Contrôle	1110	CF End
01	Contrôle	1111	CF End et CF-ACK
10	Données	0000	Données
10	Données	0001	Données et CF-ACK
10	Données	0010	Données et CF-Poll
10	Données	0011	Données, CF-ACK et CF-Poll
10	Données	0100	Fonction nulle (sans données)
10	Données	0101	CF-Ack (sans données)
10	Données	0110	CF-Poll (sans données)
10	Données	0111	CF-ACK et CF-Poll (sans données)
10	Données	1000-1111	Réservés
11	Réservé	0000-1111	Réservés

- **ToDS** (pour le système de distribution) : ce bit est mis à 1 lorsque la trame est adressée au Point d'Accès pour qu'il l'a fasse suivre au DS (Distribution System). Ceci inclut le cas où le destinataire est dans la même cellule et que le Point d'Accès doit relayer la trame. Le bit est à 0 dans toutes les autres trames.

- **FromDS** (venant du système de distribution) : ce bit est mis à 1 quand la trame vient du DS.

- **More Fragments** (d'autres fragments) : ce bit est mis à 1 quand il y a d'autres fragments qui suivent le fragment en cours.

- **Retry** (retransmission) : ce bit indique que le fragment est une retransmission d'un fragment précédemment transmis. Ceci sera utilisé par la station réceptrice pour reconnaître des transmissions doublées de trames, ce qui peut arriver si un paquet d'accusé de réception se perd.

- **Power Management** (gestion d'énergie) : ce bit indique que la station sera en mode de gestion d'énergie après la transmission de cette trame. Ceci est utilisé par les stations changeant d'état, passant du mode d'économie d'énergie au mode active ou le contraire.

- **More Data** (d'autres données) : ce bit est également utilisé pour la gestion de l'énergie. Il est utilisé par le Point d'Accès pour indiquer que d'autres trames sont stockées pour cette station. La station peut alors décider d'utiliser cette information pour demander les autres trames ou pour passer en mode actif.

- **WEP** (sécurité) : ce bit indique que le corps de la trame est chiffré suivant l'algorithme WEP.

- **Order** (ordre) : ce bit indique que cette trame est envoyée en utilisant la classe de service strictement ordonné (Strictly-Ordered service class). Cette classe est définit pour les utilisateurs qui ne peuvent pas accepter de changement d'ordre entre les trames unicast et multicast.

Durée / ID

Ce champ à deux sens, dépendant du type de trame :

- pour les trames de polling en mode d'économie d'énergie, c'est l'ID de la station
- dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV.

Les champs adresses

Une trame peu contenir jusqu'à 4 adresses, selon le bit ToDS et FromDS définit dans le champ de contrôle, comme suit :

Adresse 1 est toujours l'adresse du récepteur (ie. la station de la cellule qui est le récepteur imsupportt du paquet). Si ToDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station.

Adresse 2 est toujours l'adresse de l'émetteur (ie. celui qui, physiquement, transmet le paquet). Si FromDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station émettrice.

Adresse 3 est l'adresse de l'émetteur original quand le champ FromDS est à 1. Sinon, et si ToDS est à 1, Adresse 3 est l'adresse destination.

Adresse 4 est utilisé dans un cas spécial, quand le système de distribution sans fil (Wireless Distribution System) est utilisé et qu'une trame est transmise d'un Point d'Accès à un autre. Dans ce cas, ToDS et FromDS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire.

La table suivante résume l'utilisation des différentes adresses selon les bits FromDS et ToDS :

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

Contrôle de séquence

Le champ de contrôle de séquence est utilisé pour représenter l'ordre des différents fragments appartenant à la même trame, et pour reconnaître les paquets dupliqués. Il consiste en deux sous-champs, le numéro de fragment et le numéro de séquence qui définissent le numéro de trame et le numéro du fragment dans la trame.

Cyclic Redundancy Check

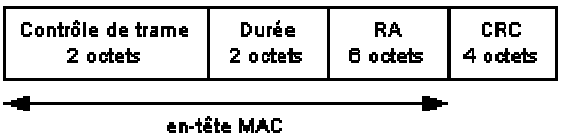
Le CRC est sur 32 bits.

Format des trames les plus courantes

Format des trames RTS

RA est l'adresse du récepteur imsupportt de la prochaine trame de données ou de gestion.
TA est l'adresse de la station qui transmet la trame RTS.
La valeur de la durée est le temps, en microsecondes, nécessaire à la transmission de la trame de gestion ou de données suivante, plus une trame CTS, plus une trame ACK, plus 3 intervalles SIFS.

Format de la trame CTS



RA est l'adresse du récepteur de la trame CTS, directement copiée du champ TA de la trame RTS.
La valeur de la durée est la valeur obtenue dans la trame RTS, moins le temps de transmission, en microsecondes, de la trame CTS et d'un intervalle SIFS.

Format de la trame ACK

RA est le champ directement copié du champ Adresse 2 de la trame précédent cette trame ACK.
Si le bit More Fragment était à 0 dans le champ de contrôle de trame de la trame pécédente, la valeur de la durée est mise à 0. Sinon, c'est la valeur du champ durée précédent, moins le temps, en microsecondes, demandé pour transmettre la trame ACK et l'intervalle SIFS.

PCF : Point Coordination Function

En plus de la fonction de base de coordination distribuée (DCF), il y a la fonction optimal de coordination par point (PCF) qui peut être utilisée pour implémenter des services temps réel, comme la transmission de voix ou de vidéo. Cette PCF fait qu'on utilise des priorités supérieures que le Point d'Accès peut gagner en utilisant des temps inter-trames plus petit (PIFS).
En utilisant un accès par priorité supérieure, le Point d'Accès peut envoyer des données aux stations en réponse à une Polling Request, tout en contrôlant l'accès au support. Pour permettre aux stations classiques d'avoir accès au support, il y a une condition qui est que le Point d'Accès doit laisser suffisamment de temps DCF par rapport au PCF.

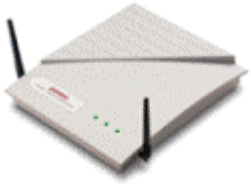
Réseaux ad hoc

Quelquefois, les utilisateurs peuvent avoir envie d'avoir un réseau local sans fil sans infrastructure (surtout sans Point d'Accès). Ceci peut permettre le transfert de fichiers entre deux utilisateurs d'agenda ou pour une rencontre hors de l'entreprise.
Le standard 802.11 répond à ce besoin par la définition du mode d'exécution « ad hoc ». Dans ce cas, il n'y a pas de Point d'Accès, et une partie de ses fonctionnalités sont reprises par les stations elles-mêmes (comme les trames balise pour la synchronisation). D'autres fonctions ne sont pas utilisables dans ce cas (relayage des trames ou mode d'économie d'énergie).

24 Mbps doivent être impérativement implémentés sur tous les produits.

Le prix des équipements : décembre 2000

Air Connect, de 3Com
Interfaces : 10Base-T, port console RS 232
Assignation d'adresse : DHCP client, port console
Administration : Telnet, émulation terminal, SNMP, HTTP
Support snmp : SNMP v1, MIB II, MIB 3Com
Prix indicatif de l'AP : 8 300 F
Prix indicatif de la carte PCMCIA : 1 700 F



WL400, de Compaq
Interfaces : 10Base-T, port console RS 232
Assignation d'adresse : interface propriétaire
Administration : interface propriétaire
Prix indicatif de l'AP : 6 900 F
Prix indicatif de la carte PCMCIA : 1 500 F

Range Lan-DS, de Proxim
Interfaces : 10/100Base-T, port console RS 232, port PCMCIA
Assignation d'adresse : DHCP client, port console
Administration : Telnet, émulation de terminal, SNMP, HTTP
Support SNMP : MIB I, II, MIB 802.11
Prix indicatif de l'AP : 8 300 F
Prix indicatif de la carte PCMCIA : 1 500 F

Aironet 340, de Cisco
Interfaces : 10/100Base-T, port console RS 232
Assignation d'adresse : DHCP client, Boot P
Administration : Telnet, FTP, SNMP, HTTP, émulation de terminal
Prix indicatif de l'AP : 9 600 F
Prix indicatif de la carte PCMCIA : 1 850 F

La norme 802.11 dans la presse

Réseaux & Télécoms : articles de l'année 2000

802.11b : des promesses à confirmer
« Compaq, Cisco, 3Com, Proxim : quatre réseaux sans fil prêts à l'emploi répondant aux recommandations 802.11b ont travaillé de concert. L'apparente liberté de choix offerte par leur garantie d'interopérabilité est fortement restreinte par une absence totale d'outils d'administration interplates-formes. […]
Au sein de la déjà ancienne norme 802.11, quelques appareils d'origine diverse acceptaient déjà de dialoguer, mais dans un mode si dégradé qu'il n'était pas rentable d'espérer une certaine interopérabilité. Le Weca (Wireless Ethernet Compatibility Alliance) allait-il gommer ces disparités ? La réponse est toute en nuances : oui et non. Oui, tous les équipements frappés du sceau 11b acceptent d'être intégrés dans un même réseau. Non, il n'est pas humainement possible de gérer un parc réellement hétérogène, faute de logiciels d'administration unifiés, d'API communes, de procédures d'installation semblables, d'interfaces physiques normées. […]
Si, en architecture cuivre, l'installation d'un hub ou d'un routeur peut s'accommoder d'une armoire ou d'une étagère proche de la baie de brassage, la mise en place d'un point d'accès, quant à elle, est bien plus complexe. Le comportement de l'Ethernet sans fil nouvelle génération ne semble apporter aucune amélioration par rapport à l'ancien 802.11. A ce sujet, 3Com offre une documentation très didactique et précise, qui recommande de bien dégager le concentrateur des masses métalliques et propose d'accrocher l'AP au plafond du local. Faux plafond obligatoire donc, pour y acheminer à la fois les câbles d'alimentation et de liaison RJ45. Encore faut-il disposer d'une prise secteur dans l'immédiate proximité de l'AP. 3Com, toujours, propose un boîtier d'alimentation de l'AP via le câble Ethernet, solution élégante mais exigeant un câblage propre. […]
Lorsque quatre clients tentent de joindre un serveur, le débit maximal dépasse rarement 3 Mbit/s. Viennent ensuite les brouillages extérieurs. Les connecteurs PCMCIA des ordinateurs portables tenant, le plus souvent, dans un mouchoir de poche, il est vain d'espérer faire cohabiter une carte 802.11b et une extension Bluetooth. Aucune transmission n'est alors possible. Deux portables équipés respectivement d'une carte Bluetooth et 802.11b se perturbent mutuellement s'ils sont placés côte à côte, et la distance minimale entre les deux émetteurs doit dépasser un bon mètre pour éliminer toute perturbation électromagnétique - ce qui ne résout pas les problèmes de collision. Viennent enfin les interférences hors bande. Celles des téléphones cellulaires en harmonique 3, brèves, peu destructrices, mais qui provoquent quelques nack lors de transmissions de fichiers. […]

Comme, dans le cadre des interfaces d'administration, rien ne donne accès à un contrôle approfondi des paramètres de cryptage, il a été impossible d'utiliser le mode Wep en mode hétérogène. Au sein d'une même marque, les protocoles de sécurité fonctionnent sans problème mais dégradent sensiblement les taux de transmission. L'usage d'un tunnel logiciel associé à une couche de compression s'avère bien plus rentable, tant sur le plan de l'interopérabilité que sur celui de l'efficacité.

Le prix de l'interopérabilité
« Partant du principe que le suffixe "b" signifie interopérable, on peut légitimement espérer ne plus tenir compte de l'origine des équipements et acheter les équipements 802.11b comme on le ferait avec un adaptateur Base-T. Liberté d'autant plus appréciable que les tarifs varient presque du simple au double d'un constructeur à l'autre : près de 1 500 francs pour une carte PCMCIA chez 3Com ou Compaq, un peu moins de 3 000 francs chez Cisco. Les prix des points d'accès sont aussi très fluctuants, de 7 000 à 10 000 francs. Ce qui conduit chaque administrateur à choisir un mode de fonctionnement particulier : soit jouer la carte de l'interopérabilité en ne recherchant que les équipements les moins chers, soit n'opter que pour une seule marque afin de tirer le meilleur parti des fonctions propriétaires du réseau si les applications utilisées exigent une bande passante élevée. »

Quand 802.11b fait l'unanimité
« La norme de réseau local sans fil 802.11b pénètre le tissu économique français. Avec 11 Mbit/s de débit et 100 m de portée, elle facilite la mobilité des personnes et peut même relier des bâtiments distants. […]

Internet fleurit au Printemps
« Les magasins Printemps développent le commerce électronique interactif. […] Le vendeur porte une caméra capable de diffuser sur le web. Monté sur des rollers, il a dans les mains un PC portable et, sur l'épaule, une webcam. […]
"A l'ouverture, nos webcamers dialoguaient avec les clients via GSM. Nous avions un accord avec un opérateur." Mais l'homme au parler franc explique qu'ils ont dû abandonner ce mode de transmission : "Le système, instable, coupait les communications et n'acceptait pas d'appels simultanés. Le débit de 9,6 kbit/s, trop lent, générait des files d'attente trop longues." Le webcamer transmet de la vidéo et du texte. Bruno Teboul se tourne alors vers une technologie de réseau local sans fil et teste la solution Airconnect 802.11b de 3Com, disponible en France depuis septembre 2000. Avec 11 Mbit/s de débit et 100 m de portée, elle correspond mieux à ses attentes. Trois jours de test ont suffi pour prouver que la technologie remplissait son rôle. Cinquante-cinq points d'accès sont déposés dans les faux plafonds des trois magasins afin de fournir une couverture sans trou du service. […]
La portée promise est là, et la liaison fonctionne d'un étage à l'autre. Sur le papier, chaque station de base peut supporter jusqu'à soixante-trois clients simultanés. »

EM Lyon : Une installation sans fil à retordre
Un réseau sans fil couvre les 25 000 m2 du campus de l'école lyonnaise. […]
Deux bornes ont été installées sur 400 m2 pour tester la solution Waveport 2, 802.11b, avec trente postes. Résultat, dans les escaliers, dans les ascenseurs, entre les salles de cours, ça marche ! Trente bornes au total ont donc été implantées sur quatre étages et alimentent deux cents postes. La portée théorique est de 300 m, mais, soumis à une obligation de haute qualité de service fixée par l'école, Yannick Bouchet a installé les bornes suivant un maillage très fin (tous les 10 m environ). […]
Autre avantage, le débit de 11 Mbit/s supporte des applications de netmeeting ou d'e-learning. […]
"Pour trente postes, le coût de mise en oeuvre est moitié moindre", souligne Yannick Bouchet. […]
"Nous avons toujours besoin d'un réseau filaire pour échanger de gros débits (100 Mbit/s), pour des applications vidéo par exemple, et nous avons conservé aussi des bornes à infrarouge pour les utilisateurs qui ne sont pas équipés pour le mobile."
Le réseau sans fil est totalement complémentaire du réseau filaire. […] »

Mairie de Lescar : Adieu Numéris, et vive le sans-fil !
« Une mairie béarnaise opte pour une solution Aironet de Cisco.
[…] Après l'étude de différentes options techniques pour remplacer ses liaisons Numéris, comme les faisceaux hertziens ou la pose de fibre optique entre les bâtiments, la mairie de Lescar a choisi une solution 802.11b parce qu'elle était la plus économique. "Au moment de l'étude, courant 1998, nous avons éliminé l'option fibre optique en raison de son coût par mètre de 40 francs, hors pose et hors équipements, trop prohibitif. Quant aux solutions de liaisons Transfix ou de faisceaux hertziens à 2 Mbit/s proposées par France Télécom, il fallait compter des frais d'installation de 72 000 francs toutes taxes comprises, et un coût variant entre 48 000 et 80 000 francs toutes taxes comprises par an et par site !", s'insurge Carole Nozères. En comparaison, les produits Aironet étaient si compétitifs que la mairie a décidé de relier ses neuf sites distants pour une addition de 285 000 francs toutes taxes comprises. La gamme de ponts Aironet 340 de Cisco, utilisés par la mairie, promet ainsi, en théorie et selon les antennes, une portée de 5,5 km à 11 Mbit/s, voire de 10,5 km à 2 Mbit/s ! […]
Côté installation, elle est simple si on respecte quelques contraintes : absence d'obstacle entre deux antennes et distance maximale de 30 m entre l'antenne installée sur le toit et le pont Aironet 340. Ensuite, il suffit de raccorder les ponts au réseau local via une interface RJ45 Ethernet à 10 Mbit/s. "L'installation complète d'un équipement sur un site dure environ une journée. Mais avant de s'engager, il est important de vérifier l'aspect juridique, car les réseaux sur la bande de fréquence 2,4 GHz sont réglementés par l'arrêté ministériel du 24 juillet 1995. Certaines communes ne peuvent installer ce type de solution, car l'armée se réserve le droit d'utiliser cette bande..."

Le Monde Informatique : 14 février 2001

Les failles de sécurité des WLAN aux normes 802.11
« Les réseaux sans fil au standard 802.11 ne sont pas sûrs. […] Le protocole WEP pêche surtout par le fait qu'il n'assure pas la sécurisation de la distribution des clés d'encryptage. […] Seul 3Com prétend proposer une solution d'individualisation des clés. Le hic, c'est que l'on quitte la norme. […] A noter que les utilisateurs d'un réseau 802.11 voient leur débit utile réduit de 20% si le cryptage est réalisé par un logiciel. Il convient d'utiliser des cartes qui assurent le cryptage au niveau matériel. »

-= From guill.net =-

Hiperlan 2 : High Performance Radio LAN version 2

Introduction

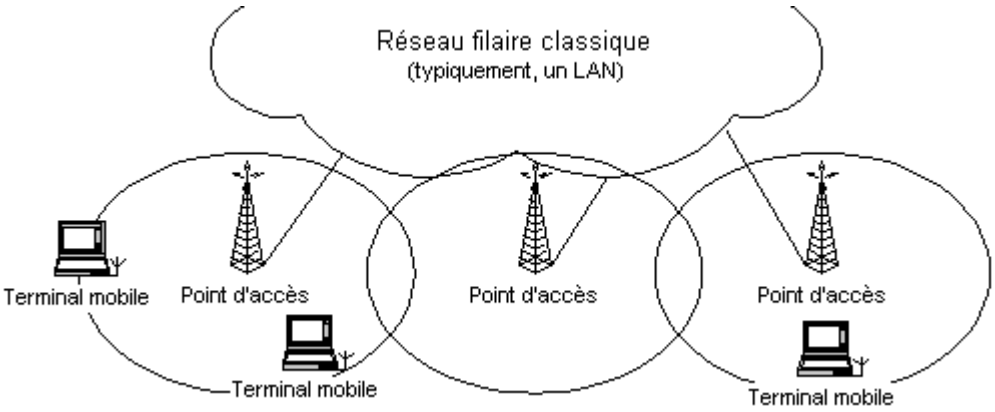
Ce standard de WLAN a été défini dans sa version 1 par le comité RES-10 du projet BRAN (Broadband Radio Access Networks) de l'ETSI le 16 juillet 1998.

Dans cette première version, les communications peuvent se faire sur 5 canaux distinctes de priorité différente. L'adaptation du CSMA/CD appelée EY-NPMA (Elimination Yield None Preemptive Priority Multiple Access) consiste à scruter les canaux par ordre de priorité jusqu'à trouver un canal libre pour émettre.
Le niveau 2 du modèle OSI est divisée en deux sous-couches, la sous-couche CAC (Channel Access Control) qui correspond à la partie physique de la technique d'accès (gestion des problèmes liés au canal hertzien ainsi que toute la transmission et réception) et la sous-couche MAC qui correspond à la partie logique, soit la mise en forme de la trame, le routage interne, les algorithmes de confidentialité, la gestion de priorité (QoS) et l'insertion et le retrait des stations.

Hiperlan 2 est soutenu par l'H2GF (Hyperlan 2 Global Forum) fondé en 1999 par Bosch, Dell, Ericsson, Nokia, Telia et Texas Instrument. Ils ont été rejoints un an après par d'autres industriels, tels Canon, Motorola ou encore Samsung. Les géant Cisco, Intel, Lucent ou Nortel sont toujours absent de ce forum. Cette deuxième version propose un débit de pointe à 54 Mbps et utilise, au niveau physique, le protocole OFDM, de la même façon que 802.11a.

Généralités

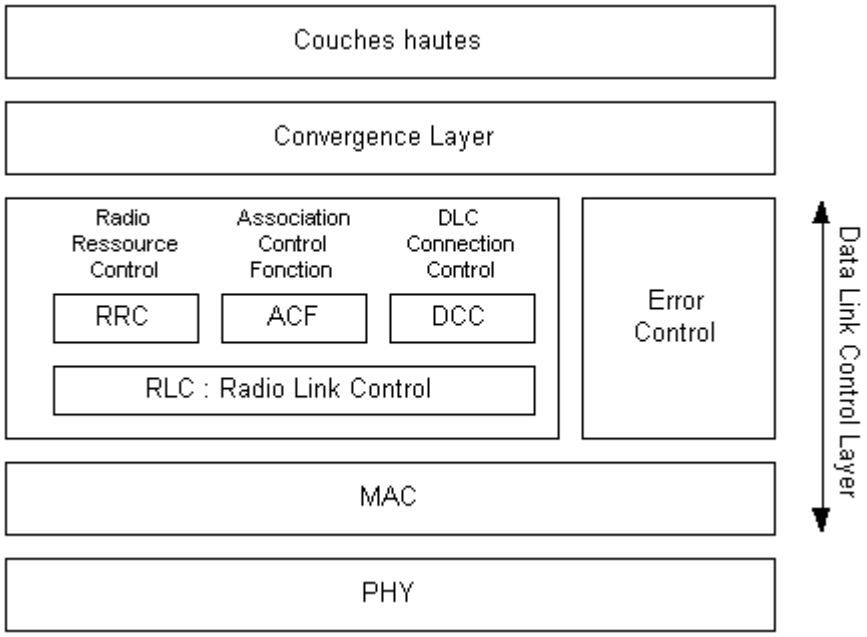
Un réseau Hiperlan 2 a généralement la topologie suivante :



Le mode ad hoc est également défini, mais n'en est qu'à sa phase primaire de développement et ne sera pas évoqué ici. Chaque terminal mobile se rattache au point d'accès dont il reçoit le meilleur signal et ne discute qu'avec ce dernier.

Les fonctionnalités offertes par Hiperlan 2 sont les suivantes :
- Haut débit : la couche physique peut transmettre et recevoir des données à 54 Mbps grâce à la modulation OFDM : Orthogonal Frequency Digital Multiplexing.
- Mode orienté-connexion : avant chaque envoi, une connexion est établie entre les MT (terminaux mobiles) et l'AP (point d'accès). Les communications point-à-point sont bidirectionnelles et les communications point-à-multipoint sont unidirectionnelles. Un canal de broadcast permet de joindre tous les MT en même temps.
- QoS : du fait que les communications sont en mode connectés, la QoS est facilement implémentable. La QoS et le haut débit offrent la possibilité de faire transiter tous types de données, de la vidéo aux données.
- Allocation automatique de fréquence : les canaux radio utilisés sont automatiquement choisis par le point d'accès en fonction des interférences dans l'environnement et des fréquences utilisées par les autres cellules radio qui l'entourent.
- Sécurité : la norme supporte l'authentification et le chiffrement des données.
- Mobilité : le MT reçoit ces données du point d'accès le mieux situé par rapport à lui, c'est-à-dire dont le signal radio est le plus intelligible. Le changement de cellule (roaming) se fait automatiquement.
- Indépendance vis-à-vis du réseau : la pile de protocole Hiperlan 2 est flexible et s'adapte facilement à tout type de réseaux et d'applications.
- Economie de batterie : la norme définit des états de puissance minimale et un mode veille.

Architecture d'Hiperlan



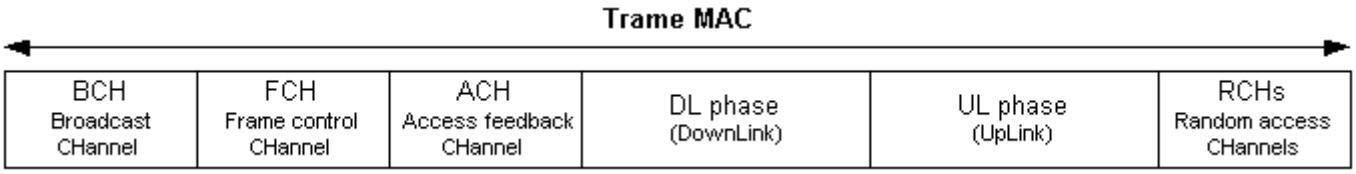
La couche physique utilise la modulation OFDM dans la norme Hiperlan 2. Les débits théoriques sont de 54 Mbps. La norme Hiperlan 1 utilise la modulation GSMK pour des débits de 1 à 2 Mbps.

Data Link Control Layer

La couche DLC (Data Link Control) fait le lien entre les points d'accès et les terminaux mobiles. Elle inclut les fonctions d'accès au média, de transmission et de gestion de la connexion.

La couche MAC

Le protocole MAC permet l'accès au média. Une trame MAC définit une période de temps précise au cours de laquelle a lieu plusieurs communications. Le point d'accès contrôle les transmissions et informe les terminaux de l'instant précis où ils sont autorisés à envoyer leurs données. La structure en cellules du média permet d'envoyer du trafic montant (uplink) et descendant (downlink) dans une même période. Ces périodes sont gérées par le point d'accès en fonction des besoins exprimés par chaque terminal.
La trame MAC est fixée à 2 ms et intègre les canaux de transport pour le broadcast, le contrôle de la trame, les contrôles d'accès, les transmissions montantes ou descendantes. Chacune de ces transmission a lieu à des instants précis.



Les différents canaux de transport sont :
- **Broadcast channel** : dans le sens descendant seulement, ce canal contient les informations de contrôle envoyées à chaque trame MAC à tous les terminaux mobiles. Ces informations sont entre autre les puissances de transmission utilisées, la longueur des canaux FCH et RCH, ou les identifiants du réseau et du point d'accès.
- **Frame control channel** : dans le sens descendant seulement, cette partie contient la description exacte de la façon dont les ressources (champs DL, UL et RCH) ont été alloués dans la trame MAC.
- Access feedback channel : dans le sens descendant seulement, donne des informations sur les demandes de ressources effectuées dans les RCH précédents.
- **Downlink et uplink phase** : bidirectionnel, il s'agit d'un train de PDU montant ou descendant. Chaque terminal ayant des données à transmettre s'est vu assigné un PDU dans le FCH. Les PDU utilisateurs sont constitués de 54 octets avec 48 octets de charge utile. Des PDU de contrôle de 9 octets sont également réservés pour accuser réception des données.
- **Random access channel** : dans le sens montant seulement, ce canal est utilisé par les terminaux effectuant une demande de ressources pour les futures trames MAC, et pour envoyer les messages de signalisation RLC.

Error Control protocol

Le mécanisme de contrôle d'erreur est utilisé pour augmenter la fiabilité de la liaison radio. Pour chaque PDU, un contrôle d'erreur a lieu, toute

erreur entraînant la retransmission du paquet. Un système d'accusés de réception est utilisé dans les phases DL et UL.

Signalisation et contrôle

Le protocole RLC (Radio Link Control) permet de gérer les terminaux et les connexions dans la cellule. Il est systématiquement associé aux protocoles ACF, DCC ou RRC.

ACF : Association Control Function

Association : Lorsqu'un terminal mobile veut rejoindre une cellule existante, il écoute les informations données par la partie BCH de la trame MAC qui vont jouer le même rôle que les trames balise de 802.11. Si la réception est correcte et que le terminal veut effectivement rejoindre la cellule, il demande un numéro d'identification (MAC-ID) au point d'accès. Ce numéro lui est accordé et il peut être intégré au réseau après une phase d'authentification.

Dissociation : Elle peut avoir lieu implicitement ou explicitement : soit le point d'accès considère la station injoignable au bout d'une certaine période de silence, soit le terminal mobile fait une demande de déconnexion du réseau. Dans les deux cas, les ressources allouées à cette machine sont libérées.

DCC : DLC user Connection Control

Ce protocole est utilisée dans la partie RCH de la trame MAC pour demander l'ouverture d'une connexion avec une autre machine. Les machines sont adressées par leur MAC-ID. Si la connexion est possible, le point d'accès répond par l'intermédiaire du canal ACH. Pour chaque connexion, un identifiant de connexion est alloué par le point d'accès.

RRC : Radio Ressource Control

Ce protocole gère deux fonctions distincts :
- Le handover (changement de cellule d'un terminal) et donc la ré-association à une autre cellule Hiperlan 2. Le point d'accès peut d'ailleurs demander explicitement à un terminal de scruter d'autres fréquences pour voir si un autre point d'accès ne serait pas plus approprié.
- L'économie d'énergie : les mises en veille et le réveil des différents terminaux.

Convergence Layer

La couche dite de convergence a deux fonctions principales : l'adaptation des services demandés par les couches hautes aux services proposés par la couche DLC, et toute la partie fragmentation, réassemblage et bourrage, afin d'adapter les trames de n'importe quel réseau pour le transport sur le réseau Hiperlan 2.

Réseau domestique électrique

Au niveau domestique, l'utilisation du réseau électrique s'affirme comme un grand concurrent des WPAN. Cette technologie, appelée PLT (Power Line Telecommunications), existe soit en réseau d'Accès (pour couvrir les dernières centaines mètres entre le transformateur basse tension – moyenne tension de 130 V et les différents domiciles), soit au niveau résidentiel, où l'on effectue des transfert à l'intérieur d'une habitation entre une prise de courant et une autre.

Cette dernière solution intéresse particulièrement les industriels. En moyenne, les habitation sont équipés de 30 prises de courant. Il s'agit de faire communiquer entre eux des ordinateurs, où n'importe quel appareil ménager. Techniquement, on superpose un signal radio très haut en fréquence (entre 1,6 et 30 MHz) sur la ligne électrique. En prenant un modem autonome, on entre d'un côté en USB ou 10baseT, puis on ressort sur une autre prise de courant, ailleurs dans la maison, sur un autre modem du même type. Cette solution est très simple : le modem est acheté en grande surface, cela évite d'ajouter un câble supplémentaire, de faire des travaux ou de faire intervenir du personnel qualifié.

Le problème qui existe actuellement est purement réglementaire : les normes européennes ne sont pas encore finies et sont en cours de discussion au sein de l'ETSI et du PLT Forum. La tâche est difficile car beaucoup d'acteurs demande des précautions.

Les militaires et radioamateurs sont contre l'utilisation de la bande de fréquence proposée actuellement. De plus, les bandes de services diffèrent d'un pays à un autre entre les différents réseaux de secours ou autre. Les câbles électriques ne sont pas blindés et rayonnent, ce qui pose un problème de CEM et radio. Une norme doit donner une énergie pas trop réduite pour faire passer l'information, et pas trop haute pour éviter de rayonner. Actuellement, il y a des négociations en cours.

Les distances peuvent sembler courtes, mais dans une maison, les 50 mètres sont facilement atteints. Pour aller d'une chambre à une autre, dans les nouvelles maisons, les deux chambres sont généralement sur des fusibles différents et il faut donc faire 2 fois l'aller-retour, sans compter les quantités de tours de portes.

Dans ce domaine, on commence tout juste à éclaircir le problème de la qualité de service. Certains tests atteignent des débits de 7,5 Mbps net en IP (soit 13 Mbps en débit brut). Cependant, le débit chute parfois brutalement lorsque la ligne électrique n'est pas parfaite.

Bluetooth et HomeRF

Les deux noms qui sortent du lot des WPAN sont Bluetooth et HomeRF. Sur le site de Bluetooth, on peut lire que 2000 constructeurs les suivent, tandis que 100 seulement soutiennent le projet HomeRF. Sur le site de HomeRF, on réplique a cela en précisant que l'inscription au soutien de Bluetooth est gratuit alors que ce n'est pas le cas pour HomeRF. Les deux normes précisent clairement qu'elles mènent une véritable croisade pour unifier l'ensemble des constructeurs. Même les sacro-saints « White Papers » sont d'une mauvaise foi évidente…

Home Radio Fréquency est une norme basée sur 802.11b et DECT. Elle permet indifféremment de faire transiter des flux audio ou des données. La norme autorise des portées de 50 mètres sans utiliser d'amplificateur.

De même que Bluetooth, HomeRF travaille au niveau physique dans la bande des 2,4 GHz, avec la technologie FHSS, à raison de 50 sauts de fréquence par seconde. Le débit nominal est de 1,6 Mbps (soit 1 Mbps réel), mais les débits peuvent atteindre 10 Mbps dans la version 2.

Bluetooth

Introduction : de l'origine pacifique du nom à la guerre commerciale

Harald Blaatand, qui vécu de 910 à 986, se traduit du suédois en « Harald la dent bleue », d'où Bluetooth en anglais. Initié par Ericsson, rapidement rejoint par IBM, Intel, Nokia et Toshiba au sein du SIG (Bluetooth Special Interest Group), le but de Bluetooth est d'unifier l'ensemble des constructeurs autour d'une seule norme sans fil : elle-même. En effet, ce nordique qui a vécu il y a plus de mille ans avait réussi l'exploit d'unifier les royaumes du Danemark, de la Norvège et des vikings alors que les guerres de religions et les divisions faisaient rage en Europe.

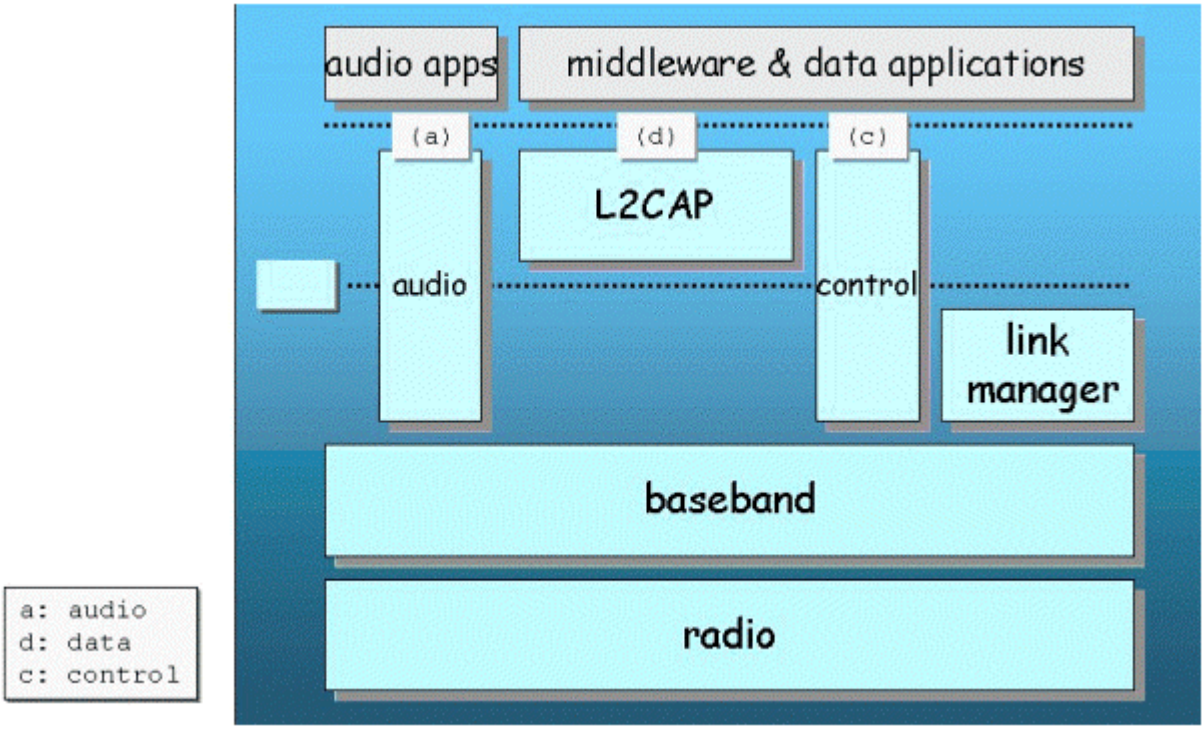
Bien sûr, l'enjeu commercial de l'époque n'était pas le même, et il n'est pas certain que l'union soit encore possible dans notre monde commercial où la hache a été remplacé par les millions… Aujourd'hui, 2400 constructeurs, dont 3Com, Motorola et

Microsoft, en plus des multinationales précédemment citées, se sont ralliés à cette cause.

Bluetooth propose de simplifier tous les problèmes de connexions en permettant à tous les périphériques et appareils distants de moins de 10 mètres (ou 100 mètres avec un amplificateur) de se connecter les uns aux autres, grâce à une puce carrée de 9mm d'arête. En 2002, Ericsson estime à plus de 100 millions le nombre d'appareils équipés de cette puce. Cette dernière coûte actuellement 20$, mais Intel prévoit qu'elle ne coûtera bientôt plus que 5$.

Le groupe de travail IEEE 802.15.1 travaille actuellement sur la normalisation de Bluetooth.

Architecture des protocoles

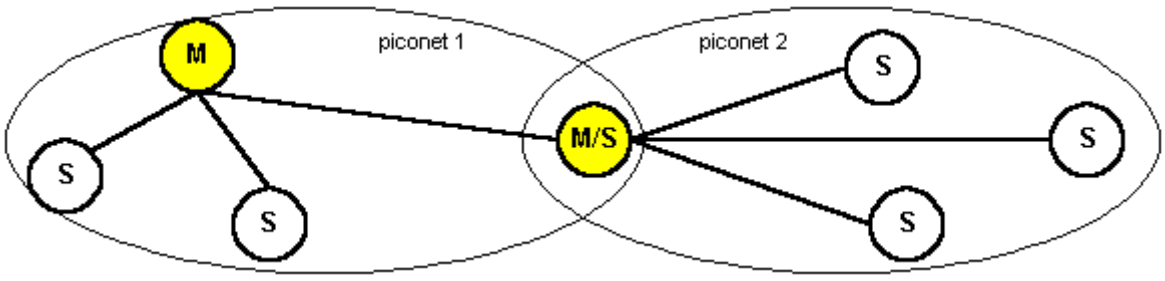


Couche physique : radio

Au niveau physique, Bluetooth utilise la technologies par saut de fréquence (FHSS) sur 79 canaux dans le bande 2,402 à 2,480 GHz. Le réseau est basé sur un système maître/esclave, et le maître décide des sauts de fréquence de façon pseudo-aléatoire, 1600 fois par seconde. La norme 1.0A définie en juillet 1999 prévoyait un débit brut de 1 Mbps (soit 720 kbps). Nul doute que ce débit sera amené à augmenter par la suite, même si la version 1.1, approuvée en mars 2001, ne le prévoit pas encore.

Les machines d'un réseau Bluetooth se rassemble en sous-réseaux appelés piconets. Dans ce piconet, une des machines joue le rôle de maître, et gère à ce titre l'horloge et les sauts de fréquence. Chaque maître peut accueillir jusqu'à 7 esclaves actifs, soit 8 appareils actifs maximum par piconet.

Plusieurs piconets adjacents constituent un scatternet et peuvent interagir. Une machine peut ainsi être esclave d'un piconet et maître d'un autre. Chaque piconet dispose d'un débit de 1 Mbps. 10 scatternets peuvent ainsi interagir, soit 72 appareils maximum (8 x 10 – 8 appareils).



Baseband layer

Cette couche permet de définir trois types de liens :
- les liaisons SCO (Synchronous Connection-Oriented) pour l'audio (ou audio et données),
- les liaisons ACL (Asynchronous Connectionless) pour les données. Dans le cas où les débits montants et descendants ne sont pas égaux, les liaisons ACL peuvent être asymétriques.
- les liaisons de base : pour toutes la gestion des connexions au sein du piconet

Les paquets ont alors la forme suivantes :

Code d'accès 72 bits	Entête 54 bits	Données 0 à 2745 bits

Le code d'accès permet la synchronisation des composants Bluetooth.
L'entête stocke le numéro de paquet, l'adresse source et destination, le type de paquet, le CRC…

Link manager protocol

Ce protocole est responsable de la supervision des différentes connexions, de l'authentification des appareils, et du chiffrement. Il gère également les mises en veille des différents appareils.

Link Layer Control & Adaptation (L2CAP)

Cette couche permet l'adaptation des protocoles supérieurs (comme TCP/IP) au réseau Bluetooth : elle supporte la segmentation et le réassemblage, et le multiplexage de protocole.

Conclusion

Sur le plan de la sécurité, des systèmes sont bien sûr en place : authentification et chiffrement jusqu'à 128 bits.
A noter que la norme Bluetooth 2 est déjà en cours d'élaboration : elle devrait étendre la portée à une centaine de mètres et autoriser des débits de 10 Mbps.

-= From guill.net =-