Les réseaux informatiques

François Preghenella

Avant propos

Le cours suivant est composé de trois niveaux de difficulté référencé comme pour les pistes de ski.


Piste bleu : la partie contient la base du cours, cette partie convient à l'option gestion de production.


Piste rouge : la partie est un peu plus poussée, elle convient aux options image, son et montage.


Piste noire : c'est la partie la plus difficile du cours, elle est prévu pour l'option TIEE, mais attention cela ne doit pas interdire les autres options de venir voir ce qui ce passe.

Bon ski dans cette descente dans la technologie.

Sommaire

1. Introduction aux réseaux locaux.

1.1. Notions sur la transmission de données.

Nous allons aborder des notions sur le vocabulaire qu'il faut connaître impérativement.
Une ligne : c'est le support physique de la communication entre deux ou plusieurs équipements.
Une voie : c'est la possibilité de transmission sur la ligne, sachant qu'une ligne peut supporter plusieurs voies.
Une liaison : c'est l'état de la communication entre deux ou plusieurs équipements.

On distingue deux types de liaisons:

- *Point à Point* : se sont deux équipements seulement qui sont reliés entre eux.
- *Multipoint* : plusieurs équipements sont reliés entre eux. Quand un message est envoyé par un équipement, tous les autres équipements le reçoivent, seul l'équipement concerné doit le prendre en compte.

Une liaison est soit permanente (établie en continue) soit temporaire et dans se cas elle est dite commutée.

On distingue deux types de commutation:

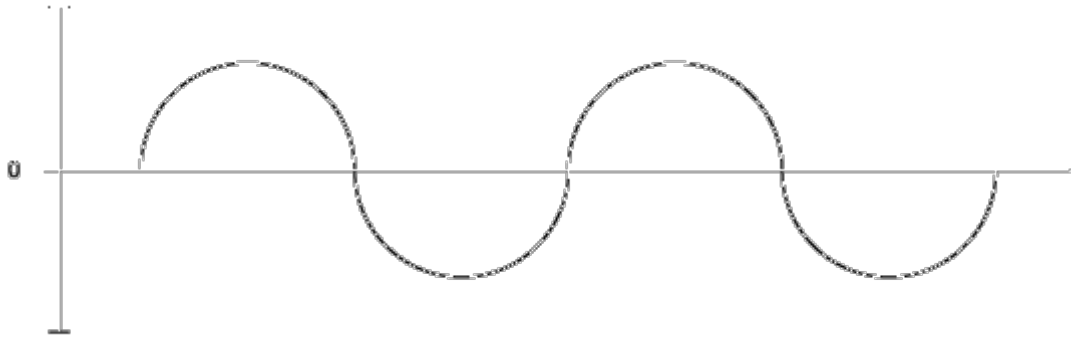
- ***La commutation de circuits (physique)*** : le chemin entre l'émetteur et le récepteur qui est assuré. La liaison n'appartient qu'aux deux interlocuteurs dès que la communication est établie. L'exemple le plus connu c'est le réseau téléphonique.
- *La commutation de messages (logique)* : c'est une commutation virtuelle dans ce cas, c'est l'acheminement de l' émetteur vers le récepteur qui est assuré.

1.2. La transmission de données.

Pour transmettre des données on utilise un signal de nature électrique puis selon un code, les codes les plus utilisés sont les codes ASCII, EBCDI, VIDEOTEX, TELEX.

Le signal analogique.
Les sons, les couleurs, la voix sont des phénomènes analogiques. Un signal est analogique quand il présente des variations continues de sa valeur entre 2 limites repérables. La transmission analogique consiste à utiliser une onde porteuse que l'on va modifier par un ou plusieurs paramètres pour exprimer les variations tel que : phase, fréquence, amplitudes.
Le réseau RTC (Réseau Téléphonique Commuté) transmet les signaux analogiques en apportant des modulations à un courant continu qui parcourt la ligne.

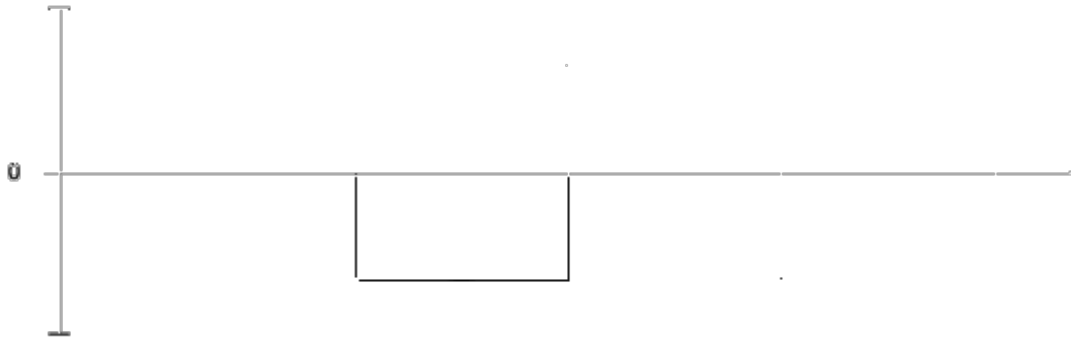
Signal analogique



Le signal numérique.

Un signal est numérique quand les valeurs peuvent prendre un nombre fini de valeurs discontinues (2 pour le signal binaire). Un signal numérique a une durée et une amplitude précises pour être transmit, si par exemple ou veut transmettre de la voix sur un réseau numérique il faut qu 'elle soit numérisée, elle est alors transcodée de l'analogique vers le numérique à l' aide de postes numériques qui assurent cette fonction.

Signal numérique



1.3. Différents modes de transmission de données.

- *La transmission série.*

Les données sont codées et transmises sur un même bus, les une à la suite des autres

- *La transmission parallèle.*

La transmission est simultanée, le parallélisme est réalisé soit par duplication de ligne, soit par le partage de la ligne.

- *La transmission synchrone.*

Dans ce mode l'intervalle de temps entre chaque donnée est constant. La synchronisation entre l'émetteur et le récepteur est assurée par une signalisation particulière qui permet de resynchroniser les horloges, l'émetteur et le récepteur sont sur la même fréquence.

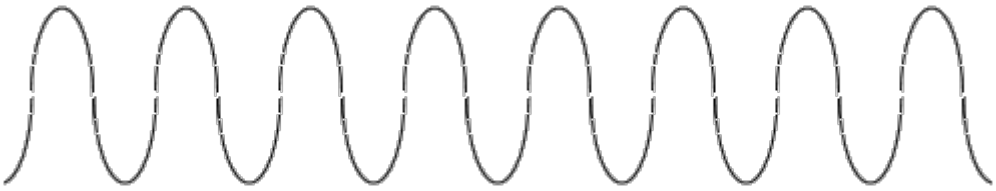
- *La transmission asynchrone.*

La fréquence peut être irrégulière, la reconnaissance des messages est réalisée par un bit start et un stop.

- *La transmission bande de base.*

En bande de base les signaux sont envoyés sous leur forme originale. Cette technique n'optimise pas la transmission car la totalité de la bande passante est occupée.

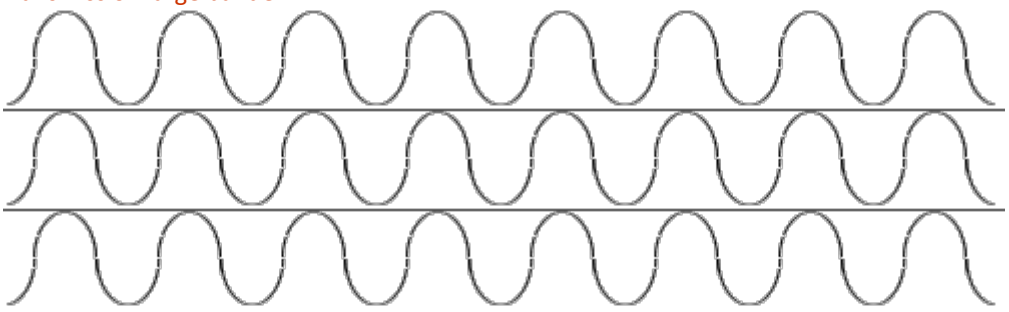
Transmission bande de base



- *La transmission large bande.*

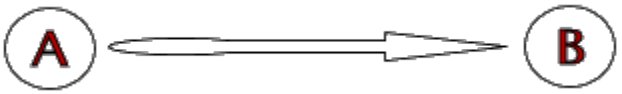
Si la voie de communication possède une large bande passante, on peut alors transmettre plusieurs ondes. La largeur de bande des raccordements téléphoniques est de 3100 Hz, mais les lignes on une bande passante de 48 Khz permettant de faire passer 12 communications en simultanées.

Transmission large bande

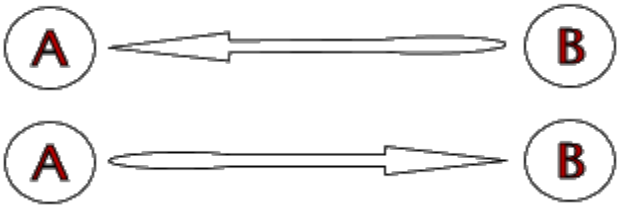


1.4. Utilisation d'une voie de transmission.

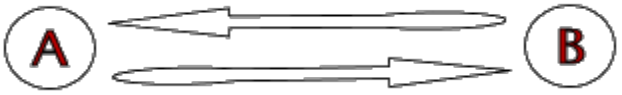
Simplex. La ligne est utilisé que dans un sens A est émetteur B récepteur.



Half Duplex. Chacun peut être émetteur ou récepteur, mais pas les deux à la fois.



Full Duplex. Chacun peut être émetteur et récepteur en même temps. La ligne est utilisée dans les 2 sens simultanément.



1.5. Le multiplexage.

Qu'est ce que les multiplexeurs (MUX) ?

Le multiplexeur est un appareil permettant le multiplexage qui consiste à regrouper sur une même ligne plusieurs voies de transport, le démultiplexage est l'opération inverse.

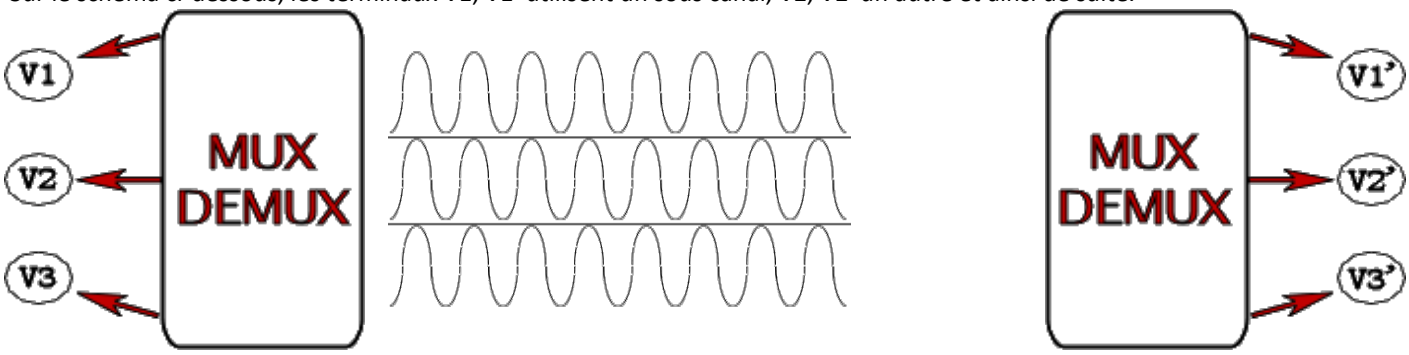
Il existe 2 grands types de multiplexage :

Les MUX fréquentiels.

Dans ce cas le multiplexage fréquentiel partage la bande de fréquence principale en sous bandes, ces nouvelles Voies sont affectées pour les Voies entrantes. Aucun adressage n'est nécessaire pour se multiplexage. Ici le signal est analogique.

Par exemple prenons le réseau téléphonique qui a une bande passante de 48 Khz divisée en 12 bandes de 3100 Hz.

Sur le schéma ci-dessous, les terminaux V1, V1' utilisent un sous canal, V2, V2' un autre et ainsi de suite.



Les MUX temporels.

Dans ce cas le multiplexage temporel alloue un intervalle de temps à chaque voie entrante. Les signaux sont numériques.

Par exemple dans le schéma ci-dessus V1, V2, V3 se voient allouer des intervalles de temps pour communiquer.

Comme la bande passante est entièrement utilisé, il est nécessaire de mettre en place un système d'adressage.

1.6. Principes de commutation.

Dans un système de transmission comme un réseau, les informations d'une communication transitent par divers nœuds (Dispositif actif sur un réseau informatique).

La commutation permet de réaliser une liaison temporaire entre l'équipement demandeur, et l'équipement demandé, et tout cela au travers d'un réseau.

Voici les différentes techniques de commutation :

- *La commutation spatiale.*

La liaison est établie de manière physique grâce à des équipements mécaniques, électromécanique ou électronique.

- *La commutation temporelle.*

Par multiplexage, plusieurs communications sont concentrées sur une même liaison physique pour en augmenter le taux d'utilisation. Des mémoires tampons dans les MUX sont nécessaires pour stocker les messages qui attendent que la liaison soit libre.

- *La commutation virtuelle (logique).*

Cette méthode est utilisée que dans la commutation de messages. Chaque message contient son adresse de destination. Ainsi, chaque nœud sur lequel le message arrive est capable de router le message vers un autre, pour enfin arriver à destination.

2. Typologie et topologie des réseaux.

2.1. Qu'est ce que la Typologie et la Topologie ?

La typologie c'est l'étude des modèles de réseaux courant, on distingue généralement deux grandes classes de réseaux :

- Les LAN ou Local Area Network (réseau local) font partie des petits réseaux localisés dans un même bâtiment ou des bâtiments proches.
- Les WAN ou Wide Area Network (réseau étendu) sont des réseaux d'entreprise et autres qui relient plusieurs sites distants les un aux autres.

La topologie c'est le terme qui désigne la disposition des éléments comme le câblage, les ordinateurs et autres composants dans un réseau. Elle montre comment les composants sont interconnectés entre eux.
On distingue :

- *La topologie physique.*

C'est la représentation des nœuds d' un réseau et les liens physiques qui existent entre eux.

- *La topologie logique.*

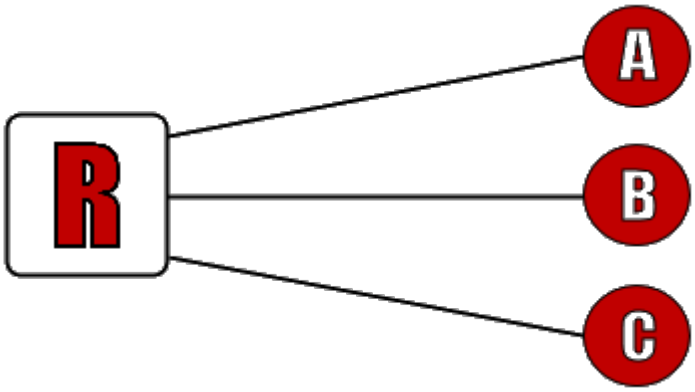
C'est le mode de circulation des données sur le câble et autres supports.

2.2. Les liaisons Point à Point.

La liaison Point à Point est la méthode la plus rudimentaire des topologies. Une liaison est en point à point si deux composants sont connectés entre eux et peuvent communiquer.

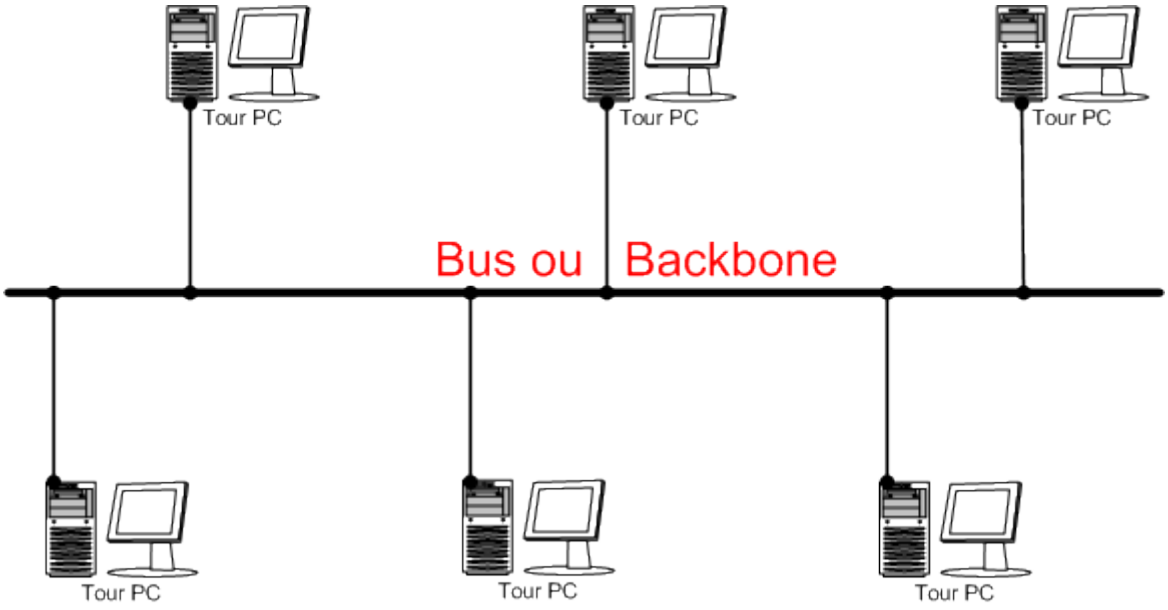
2.3. Les liaisons multipoints.

Une liaison est multipoints dès qu'un nœud principal peut communiquer avec deux dispositifs secondaires.



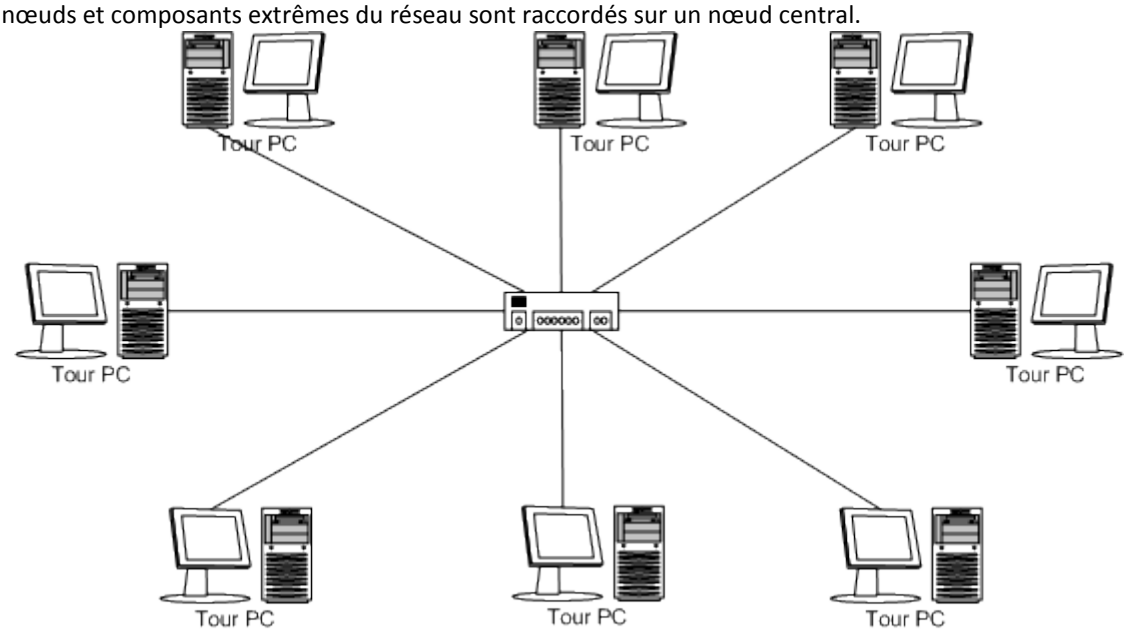
2.4. Les réseaux en bus.

Chaque nœuds et composants du réseau sont raccordés sur un même câble appelé artère principale ou Backbone.



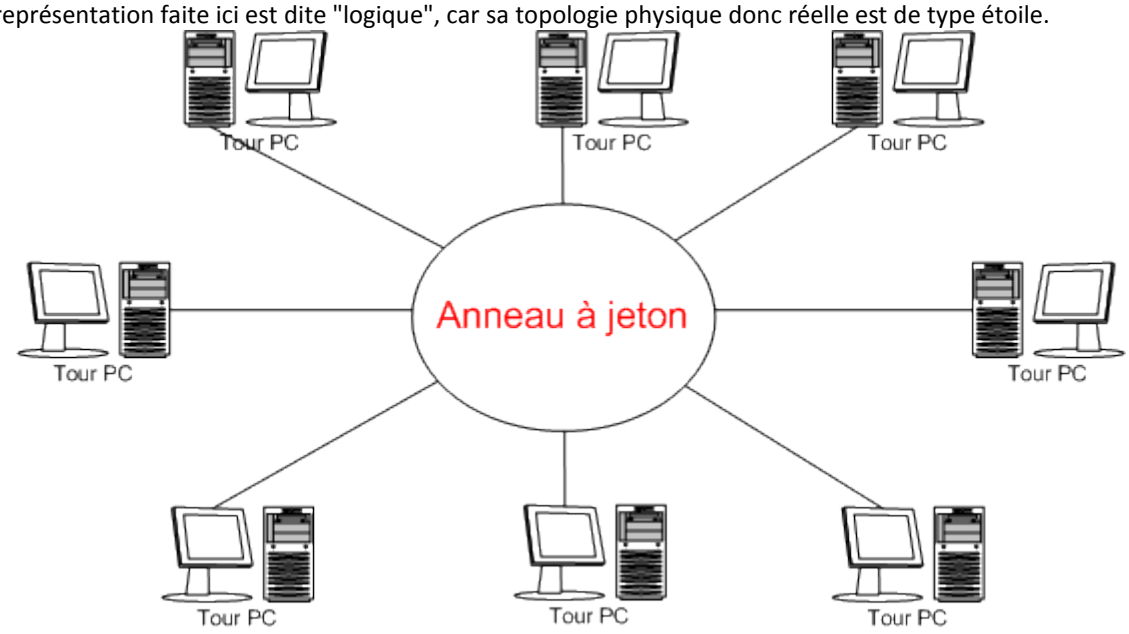
2.5. Les réseaux en étoile.

Les nœuds et composants extrêmes du réseau sont raccordés sur un nœud central.



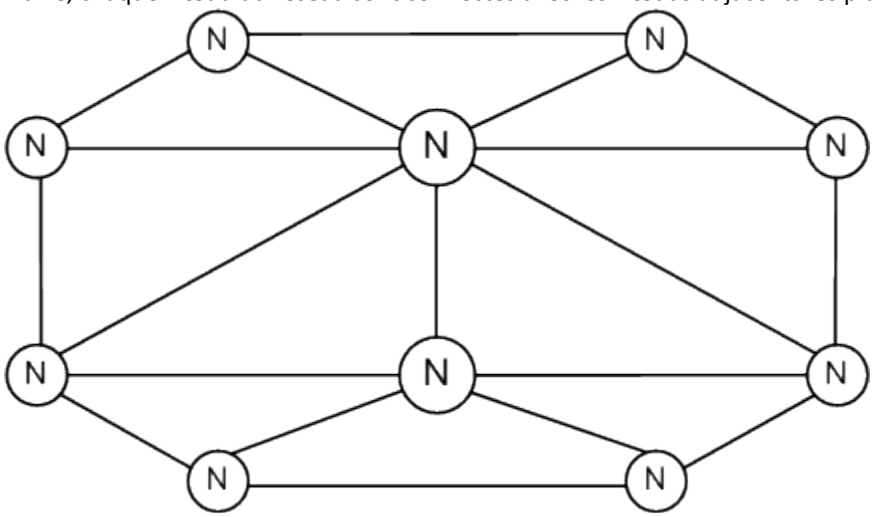
2.6. Les réseaux en anneau.

Les nœuds et composants du réseau sont les uns derrière les autres sur une boucle fermée.
La représentation faite ici est dite "logique", car sa topologie physique donc réelle est de type étoile.



2.7. Les réseaux maillés.

Dans un réseau maillé, chaque Nœud du réseau sont connectés avec les Nœuds adjacents les plus proches.



3. La normalisation des réseaux.

3.1. Qu'est ce que la normalisation ?

Un réseau met en œuvre des supports de communications faisant intervenir des matériels, des logiciels qui doivent s'entendre pour assurer les transmissions. C'est là que la normalisation doit permettre et assurer la communication entre :

- Les matériels.
- Les logiciels.
- La technologie des systèmes.

On doit pouvoir communiquer sans se préoccuper :

- Des topologies.
- Des types de lignes privées ou publiques.
- Des supports.
- Des protocoles de communication.

Il existe plusieurs organismes acteurs de la normalisation pour les réseaux.
L'ISO (International Standard Organisation) est chargé de la normalisation de tous les secteurs sauf :

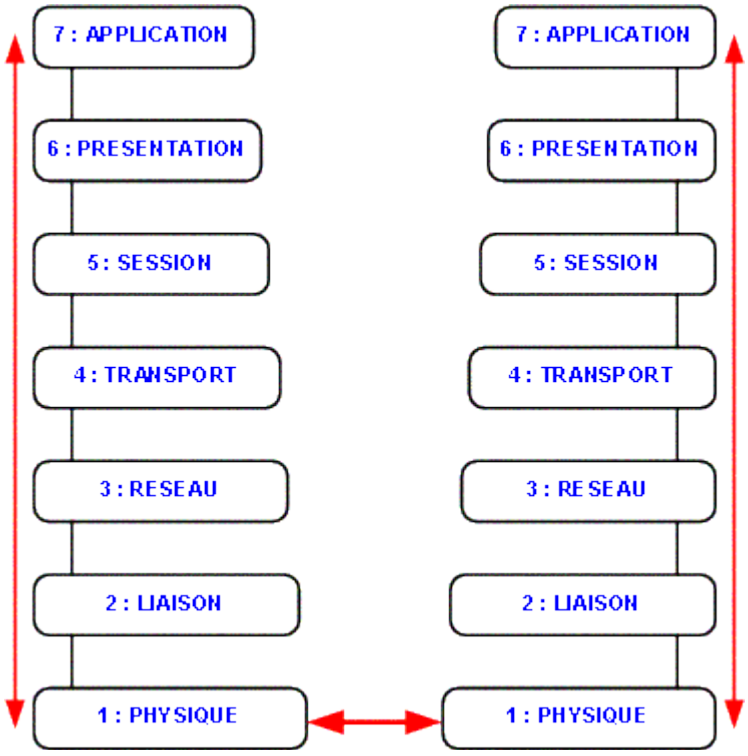
- Les télécommunications qui dépendent du CCITT (Comité Consultatif Internationale Télégraphique et Téléphonique)
- L'électricité, l'électrotechnique qui dépend du CEI (Comité Electrotechnique Internationale)

L'ANSI (American National Standards Institut) membre de l'ISO.
L'IEEE (Institute of Electrical and Electronic Engineers).
L'AFNOR (Association Française de NORmalisation)

3.2. Le modèle OSI.

Le modèle OSI (Open System Interconnection) a été élaboré par l'ISO en 1983.
Son but est de proposer aux éditeurs et aux constructeurs un modèle sur lequel ils pourront produire leurs solutions physiques. Donc en s'appuyant sur un modèle normalisé, tous produits sera ouvert aux autres systèmes qui eux aussi s'appuient sur la même norme.

Le modèle OSI

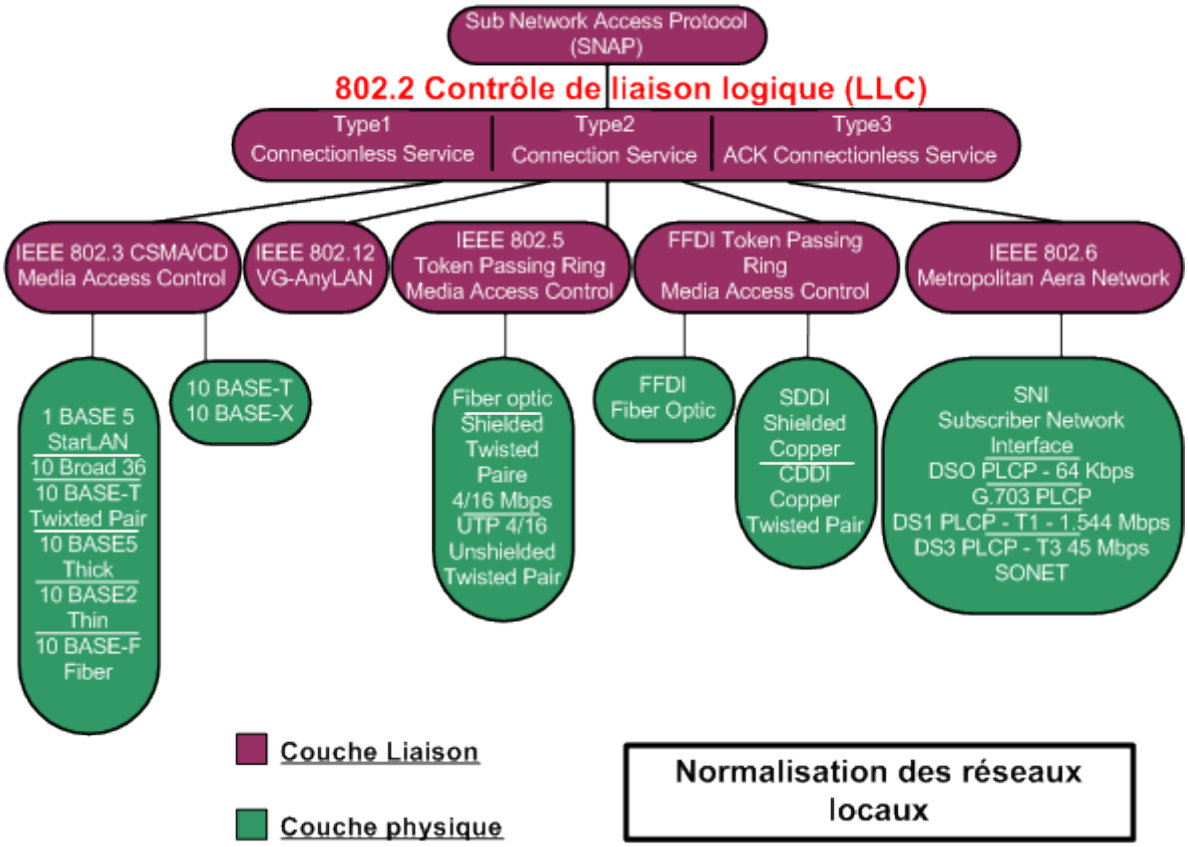


3.3. Rôle des couches.

- La couche physique : en Anglais Physical Layer, elle assure le transport des informations, c'est le lien physique entre les composants du réseau.
- La couche liaison : Line Layer en Anglais, elle est responsable de l'acheminement des blocs d'informations sans erreurs, car il se peut que le lien physique peut introduire des erreurs, ces blocs sont appelés trames.
- La couche réseau : Network Layer, elle est responsable de l'acheminement des paquets de données, elle assure l'opération d'adressage, de routage et aussi le contrôle des flux au niveau des nœuds.
- La couche transport : Transport Layer, elle est responsable du contrôle du transport de bout en bout, elle assure le découpage, le réassemblage et la cohérence des données.
- La couche session : Session Layer, elle a pour tâches la synchronisation des événements, la mise en place et le contrôle du dialogue entre les tâches distantes.
- La couche présentation : Présentation Layer, elle est responsable de la présentation ou structure des données échangées par les applications.
- La couche application : Application Layer, elle contient les modules permettant d'écrire des applications faisant appel au modèle OSI.

3.4. Les réseaux et le modèle OSI.

La normalisation est un ensemble de spécifications qui a été proposées par les entreprises comme INTEL, XEROX dans une proposition appelé ETHERNET
Deux organismes ont contribués aux travaux de normalisation des réseau locaux, L'IEEE et l'ECMA (European Computer Manufacturers Association), ils ont travaillé essentiellement sur les deux premières couches du modèle OSI, la couche physique et la couche liaison.



Le principal but de la normalisation des réseaux locaux concernait les méthodes d'accès.
Une méthode d'accès est un ensemble de règles qui définissent la manière dont ordinateur dépose et reçoit les données du câble. Les informations sont transmise sous la forme d'ensemble logiques de données appelés Trames.
Les principales méthodes sont IEEE 802.3, IEEE 802.5 et IEEE 802.12.

3.5. Les méthodes d'accès.

La méthode Ethernet CSMA/CD (Carrier Sense Multiple Access with Collision Detect) se qui donne en français : méthode d'accès multiple avec écoute de la porteuse et détection de collision. Elle est normalisée sous l'appellation 802.3
Elle consiste pour un ordinateur, au moment où il émet, à écouter si un autre est en train d'émettre. Si c'est le cas, il cesse d'émettre et réémet son message au bout d'un délai.
On qualifie cette méthode de probabiliste, en ce sens qu'on ne peut prévoir le temps nécessaire à un message pour être émis, transmis et reçu.
L'autre méthode, est celle du jeton sous la norme 802.5, est une méthode dite déterministe, car on peut déterminer le temps maximal que prendra un message pour atteindre son destinataire, tout cela en fonction des caractéristiques du réseau.

4. Les cartes réseaux

4.1. La carte réseau

La carte réseau (NAC : Network Adapter Card) constitue un composant indispensable pour la création d'un réseau informatique. Celle-ci permet la connexion d'un câble réseau établissant la liaison entre différents ordinateurs. Il existe différents types de carte réseau, mais ils possèdent tous la même vocation, à savoir, l'envoie, la réception et le contrôle des données sur un réseau.

A partir du moment où un ordinateur est équipé d'une CR et qu'il est destiné à être mis en réseau avec d'autres postes, on peut aussi dire que la CR sert de « carte d'identité »pour le poste à l'intérieur du réseau. En effet, pour être reconnu sur un réseau, un numéro appelé adresse IP (Internet Protocol) est attribué à chaque CR, ainsi il est possible de différencier tous les ordinateurs constituant un réseau. Cette adresse IP est modifiable selon le type de réseau utilisé (selon la classe). La véritable identification d'une CR se fait grâce à l'adresse MAC qui est prédéfini lors de la fabrication d'une CR du même fabricant et du même modèle.

Les cartes réseaux actuelles se connectent directement sur la carte mère via un slot (connecteur d'extension) PCI (Peripheral Component InterConnect). Il est possible de brancher plusieurs cartes réseaux sur la même carte mère.

4.2. Principes de transmission de données

Une carte réseau est munie d'un transceiver qui permet de transformer les données d'un format à un autre (format parallèle au format série) pour les envoyer sur le réseau. Ainsi les données pourront transiter à travers les câbles réseaux.

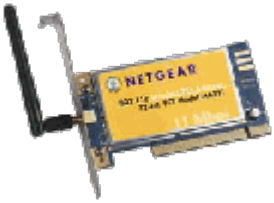
Pourquoi changer le format des données de parallèle à série :

Dans votre unité centrale, les données circulent sur ce qu'on appelle des Bus de données, ces Bus sont constitués de plusieurs « fils » mis en parallèle dans lesquels transitent vos données. A l'inverse des Bus de données, un câble réseau n'est constitué que d'un unique flux de données (c'est à dire qu'il ne peut pas envoyer et recevoir en même temps) il faut donc que la CR créée des groupes de données pour les faire transiter dans le câble. Donc les signaux numériques provenant de l'unité centrale sont transformés en signaux électriques (ou optiques pour les réseaux en fibres optiques)

Lorsqu'une CR envoie des données, elle envoie aussi sont adresse IP afin d'être identifié par l'ordinateur distant.

4.3. Différents types de cartes et débit selon les cartes :

- Les cartes standards actuelles sont les 10 Base T qui utilisent des câbles réseaux contenants des fils de cuivre torsadés (désignés par la catégorie 5, appelés aussi : paires torsadées). Les câbles de cette catégorie permettent des débits allant jusqu'à 1000 Mbits/s maximum. Les connecteurs situés aux deux extrémités du câble sont de type RJ45, il ressemble beaucoup au RJ11 (utilisé dans la téléphonie) mais est un peu plus grand et possède plus de broches (8 au lieu de 6)
- La Fibre Optique : les cartes réseaux acceptant les câbles à base de fibres optiques possèdent des avantages que n'ont pas les CR 10 Base T. En effet, elles permettent des distances plus éloignées entre deux postes (maximum 10 Km, alors que pour les 10 Base T, le segment maximum d'un câble est de 100 mètres). Ce genre de réseau est surtout utilisé pour relier des bâtiments entre eux, il ne convient pas pour les petites liaisons car son coût est élevé.
- Le WIFI : réseau sans fils (**WI** reless **FI** delity ou norme 802.11B pour 11Mb/s 802.11G pour 54Mb/s).



Comme son nom l'indique, les ordinateurs sont grâce à cette technologie interconnectés sans liaison filaire. Les CR WIFI sont dotées d'une antenne capable de recevoir des ondes radio-électriques (radio (hertziennes) et infrarouges). Plusieurs catégories de la technologie WIFI sont mises à disposition des utilisateurs, leurs différences se jouent sur la fréquence d'émission ainsi que sur débit et la portée des transmissions de données.

4.4. Catégories et normes des câbles réseaux:

• La paire torsadée :

La paire torsadée (encore appelé câblage 10 base T) ressemble au fil du téléphone et est très utilisée dans les entreprises pour les raccordements téléphoniques et informatiques. Toutefois ce câblage n'est pas blindé et si l'on veut des débits importants, il faut limiter la distance entre deux noeuds (100 mégabits par seconde (Mbits/s) pour une distance maximum de 100 mètres, 1 Mbits/s lorsque la distance est de quelques centaines de mètres). Il s'agit d'un type de câblage bon marché. Les connecteurs utilisés pour le raccordement de ces câbles sont de type RJ45.

On distingue:

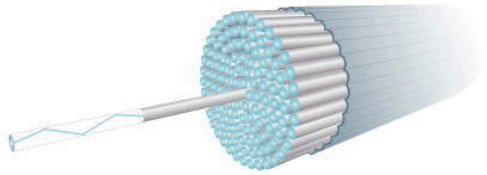
Le câble STP: Shielded Twisted Pair pour paire torsadée blindée. Ce traitement améliore les performances du câble du point de vue de l'immunité aux interférences extérieures.

Le câble UTP: Unshielded Twisted Pair pour torsadée non blindée.

Le câble FTP: Foiled Twisted Pair pour une feuille d'alu enroulée autour des paires.

Le câble SFTP: Shielded Foiled Twisted Pair

Dénomination	Caractéristique
Catégorie 1	Transport de la voix
Catégorie 2	Voix et Données 4MB/s
Catégorie 3	Voix et Données 10MB/s
Catégorie 4	Voix et Données 16MB/s
Catégorie 5	Voix et Données 100MB/s
Catégorie 6	Voix et Données 1000MB/s

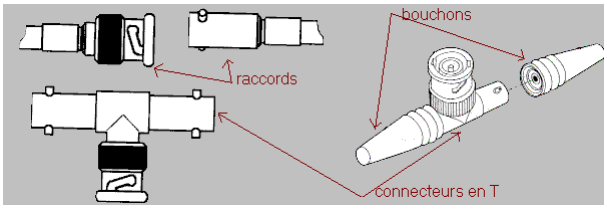


La fibre optique:

Les câbles coaxiaux tendent désormais à être remplacés par des fibres optiques en verre. Les messages sont codés numériquement en impulsions lumineuses et transmis sur de grandes distances le long de ces minces fibres. Sur ce type de support, les signaux transmis sont complètement insensibles aux rayonnements électromagnétiques, ne subissant ainsi aucune altération. Un câble à fibres optiques peut acheminer simultanément plusieurs milliers de messages. La fibre optique permet de très grandes vitesses sur de grandes distances (150 mégabits par seconde (Mbits/s) sur une dizaine de kilomètres soit 15 fois la vitesse d'un réseau local courant). Grâce à de telles vitesses, il devient possible de transmettre en temps réel des sons, et même des images animées. Ce support est encore d'un coût élevé mais tend à devenir compétitif avec le câble coaxial.

Les connecteurs utilisés pour le raccordement de ces câbles sont de type connecteur 15 broches..

• Le câble coaxial:



le câble coaxial est largement utilisé dans les réseaux de type bus. Du fait de sa conception, le signal transporté est protégé des interférences électriques et ne subit qu'une faible atténuation ce qui permet des débits relativement importants sur des distances assez grandes. On peut y acheminer un nombre important de messages simultanément. Il en existe deux types : thick (épais) ou thin (fin).

Le câblage Ethernet thin (encore appelé câblage noir ou câblage capillaire, ou câblage coaxial fin, ou encore câble 10 base 2) est peu onéreux, a un diamètre de 0,5 cm et autorise un débit de 10 mégabits par seconde et peut relier des stations distantes de 200 m.

Le câblage thick (encore appelé câblage jaune, ou câblage coaxial épais, ou câble 10 base 5) est relativement cher, lourd et peu flexible, a un diamètre de 1 cm et peut relier entre elles des stations distantes de 500 mètres.

4.5. Tableau récapitulatif des normes de câblage.

Type de câble	Connectique	Dénomination uselle	Longueur maximale	Distance entre 2 points
Paire torsadée	RJ45	10 base T	100 m	X
Coaxial épais	AUI	10 base 5	500 m	2.5 m
Coaxial fin	BNC	10 base 2	185 m	0.5 m
Fibre optique*	ST	X	de 2 à 10 KM	de 2 à 10 KM

*en fonction du type "mono" ou "multi" mode.

5. Ethernet

Ethernet est un protocole de réseau informatique à commutation de paquets implémentant la couche physique et la sous-couche Media Access Control du modèle OSI mais le protocole Ethernet est classé dans la couche de liaison, car les formats de trames que le standard supporte est normalisé et peut être encapsulé aussi dans d'autres protocoles que les couches physiques MAC et PHY de l'Ethernet, ces couches physiques faisant l'objet de normes séparées en fonction des débits, du support de transmission, longueur et conditions environnementales.
C'est au départ une technologie de réseau local permettant que toutes les machines d'un réseau soient connectées à une même ligne de communication, formée de câbles cylindriques (câble coaxial, paires torsadées). Le standard qui a été le plus utilisé dans les années 1990 et qui l'est toujours est le 802.3 de l'IEEE (maintenant aussi adopté comme norme internationale ISO/CIE 8802-3). Ce dernier a largement remplacé d'autres standards comme le Token Ring et l'ARCNET.
Le nom Ethernet vient de l'éther, milieu mythique dans lequel baigne l'Univers, et *net*, abréviation de réseau en anglais. Le réseau ancêtre ALOHAnet utilisait les ondes radiofréquences se propageant dans l'éther.

5.1. Histoire

L'Ethernet a originellement été développé comme l'un des projets pionniers du Xerox PARC. Une histoire commune veut qu'il ait été inventé en 1973, quand Bob Metcalfe écrit un mémo à ses patrons à propos du potentiel d'Ethernet. Metcalfe affirme qu'Ethernet a en fait été inventé sur une période de plusieurs années. En 1976, Robert Metcalfe et David Boggs (l'assistant de Metcalfe) ont publié un document intitulé *Ethernet : Distributed Packet-Switching For Local Computer Networks* (Ethernet : commutation de paquets distribuée pour les réseaux informatiques locaux).
Metcalfe a quitté Xerox en 1979 pour promouvoir l'utilisation des ordinateurs personnels et des réseaux locaux, et a formé l'entreprise 3Com. Il réussit à convaincre DEC, Intel et Xerox de travailler ensemble pour promouvoir Ethernet en tant que standard. Ethernet était à l'époque en compétition avec deux systèmes propriétaires, Token Ring et ARCnet, mais ces deux systèmes ont rapidement diminué en popularité face à l'Ethernet. Pendant ce temps, 3Com est devenue une compagnie majeure du domaine des réseaux informatiques.

5.2. Description générale

L'Ethernet est basé sur le principe de membres (pairs) sur le réseau, envoyant des messages dans ce qui était essentiellement un système radio, captif à l'intérieur d'un fil ou d'un canal commun, parfois appelé *l'éther*. Chaque paire est identifiée par une clé globalement unique, appelée adresse MAC, pour s'assurer que tous les postes sur un réseau Ethernet aient des adresses distinctes.
Une technologie connue sous le nom de *Carrier Sense Multiple Access with Collision Detection* (Écoute de porteuse avec accès multiples et détection de collision) ou CSMA/CD régit la façon dont les postes accèdent au média. au départ développé durant les années 1960 pour ALOHAnet à Hawaii en utilisant la radio, la technologie est relativement simple comparée à Token Ring ou aux réseaux contrôlés par un maître. Lorsqu'un ordinateur veut envoyer de l'information, il obéit à l'algorithme suivant :
Si le média n'est pas utilisé, commencer la transmission, sinon aller à l'étape 4
[Transmission de l'information] Si une collision est détectée, continue à transmettre jusqu'à ce que le temps minimal pour un paquet soit dépassé (pour s'assurer que tous les postes détectent la collision), puis aller à l'étape 4
[Fin d'une transmission réussie] Indiquer la réussite au protocole du niveau supérieur et sortir du mode de transfert.
[Câble occupé] Attendre jusqu'à ce que le fil soit inutilisé.

[Le câble est redevenu libre] Attendre pendant un temps aléatoire, puis retourner à l'étape 1, sauf si le nombre maximal d'essais de transmission a été dépassé.
[Nombre maximal d'essais de transmission dépassé] Annoncer l'échec au protocole de niveau supérieur et sortir du mode de transmission.
En pratique, ceci fonctionne comme une discussion ordinaire, où les gens utilisent tous un médium commun (l'air) pour parler à quelqu'un d'autre. Avant de parler, chaque personne attend poliment que plus personne ne parle. Si deux personnes commencent à parler en même temps, les deux s'arrêtent et attendent un court temps aléatoire. Il y a de bonnes chances que les deux personnes attendent un délai différent, évitant donc une autre collision. Des temps d'attente exponentiels sont utilisés lorsque plusieurs collisions surviennent à la suite.
Comme dans le cas d'un réseau non commuté, toutes les communications sont émises sur un médium partagé, toute information envoyée par un poste est reçue par tous les autres, même si cette information était destinée à une seule personne. Les ordinateurs connectés sur l'Ethernet doivent donc filtrer ce qui leur est destiné ou non. Ce type de communication « quelqu'un parle, tous les autres entendent » d'Ethernet est une de ses faiblesses, car, pendant que l'un des nœuds émet, toutes les machines du réseau reçoivent et doivent, de leur côté, observer le silence. Ce qui fait qu'une communication à fort débit entre seulement deux postes peut saturer tout un réseau local.
De même, comme les chances de collision sont proportionnelles au nombre de transmetteurs et aux données envoyées, le réseau devient extrêmement congestionné au-delà de 50 % de sa capacité (indépendamment du nombre de sources de trafic). Pour résoudre ce problème, les commutateurs ont été développés afin de maximiser la bande passante disponible.
Suivant le débit utilisé, il faut tenir compte du domaine de collision régi par les lois de la physique et notamment le déplacement électronique dans un câble de cuivre. Si l'on ne respecte pas ces distances maximales entre machines, le protocole CSMA/CD n'a pas lieu d'exister.
De même si on utilise un commutateur, CSMA/CD est désactivé. Et ceci pour une raison que l'on comprend bien. Avec CSMA/CD, on écoute ce que l'on émet, si quelqu'un parle en même temps que moi il y a collision. Il y a donc incompatibilité avec le mode full-duplex des commutateurs.

5.3. Types de trames Ethernet et champ *EtherType*

Il y a quatre types de trame Ethernet :
Ethernet originale version I (n'est plus utilisée)
Ethernet Version 2 ou Ethernet II (appelée trame DIX, toujours utilisée)
IEEE 802.x LLC
IEEE 802.x LLC/SNAP
Ces différents types de trame ont des formats et des valeurs de MTU différents mais peuvent coexister sur un même médium physique.
La version 1 originale de Xerox possède un champ de 16 bits identifiant la taille de trame, même si la longueur maximale d'une trame était de 1500 octets. Ce champ fut vite réutilisé dans la version 2 de Xerox comme champ d'identification, avec la convention que les valeurs entre 0 et 1500 indiquaient une trame Ethernet originale, mais que les valeurs plus grandes indiquaient ce qui a été appelé l'EtherType, et l'utilisation du nouveau format de trame. Ceci est maintenant supporté dans les protocoles IEEE 802 en utilisant l'entête SNAP.
L'IEEE 802.x a de nouveau défini le champ de 16 bits après les adresses MAC comme la longueur. Comme l'Ethernet I n'est plus utilisé, ceci permet aux logiciels de déterminer si une trame est de type Ethernet II ou IEEE 802.x, permettant la cohabitation des deux standards sur le même médium physique. Toutes les trames 802.x ont un champ LLC. En examinant ce dernier, il est possible de déterminer s'il est suivi par un champ SNAP ou non.

5.4. Ethernet en octets

0 1 2 3 4 5 6 7 8 9 10 11	12 13	14 ---------- 1513	1514 1515 1516 1517
Adresse MAC destination	Adresse MAC source	Type de protocole	Données	FCS/CRC

Attention il existe d'autres types de trames Ethernet spécifiant la longueur notamment ainsi que d'autres particularités. Avec pour le champs Type de protocole les valeurs suivantes :

0x0800 :IPv4
0x86DD :IPv6
0x0806 :ARP
0x8035 :RARP
0x0600 :XNS
0x809B :AppleTalk
Remarques :
On notera la présence parfois d'un préambule de 64 bits de synchronisation, alternance de 1 et 0 avec les deux derniers bits à 1. (non représenté sur la trame).
L'adresse de broadcast (*diffusion*) Ethernet a tous ses bits à *1*
La taille minimale des données est de 46 octets (RFC 894 - Frame Format)

5.5. Variétés d'Ethernet

La section ci-dessous donne un bref résumé de tous les types de média d'Ethernet. En plus de tous ces standards officiels, plusieurs vendeurs ont implémenté des types de média propriétaires pour différentes raisons -- quelquefois pour supporter de plus longues distances sur de la fibre optique.
Quelques anciennes variétés d'Ethernet
Xerox Ethernet -- L'implémentation originale d'Ethernet, qui a eu deux versions, la version 1 et 2, durant son développement. La version 2 est encore souvent utilisée.
10BASE5 (aussi appelé *Thick Ethernet*) -- Ce standard de l'IEEE publié très tôt utilise un câble coaxial simple dans lequel on insère une connexion en perçant le câble pour se connecter au centre et à la masse (prises *vampires*). Largement désuet, mais à cause de plusieurs grandes installations réalisées très tôt, quelques systèmes peuvent encore être en utilisation.
10BROAD36 -- Obsolète. Un vieux standard supportant l'Ethernet sur de longues distances. Il utilisait des techniques de modulation en large bande similaires à celles employées par les modems câble, opérées sur un câble coaxial.
1BASE5 -- Une tentative de standardisation de solution pour réseaux locaux à bas prix. Il opère à 1 Mbit/s mais a été un échec commercial.
Ethernet 10 Mbit/s
10BASE2 (aussi appelé *ThinNet* ou *Cheapernet*) -- un câble coaxial de 50 ohms connecte les machines ensemble, chaque machine utilisant un adaptateur en T pour se brancher à sa carte réseau. Requiert une terminaison à chaque bout. Pendant plusieurs années, ce fut le standard Ethernet dominant.
10BASE-T -- Fonctionne avec 4 fils (deux paires torsadées) sur un câble CAT-3 ou CAT-5 avec connecteur RJ45. Un concentrateur (ou hub) ou un commutateur (ou switch) est au centre du réseau, ayant un port pour chaque nœud. C'est aussi la configuration utilisée pour le 100BASE-T et le Gigabit Ethernet (câble CAT-6). Bien que la présence d'un nœud central (le hub) donne une impression visuelle de topologie en étoile, il s'agit pourtant bien d'une topologie en bus - tous les signaux émis sont reçus par l'ensemble des machines connectées. La topologie en étoile n'apparaît que si on utilise un commutateur (switch).
FOIRL -- *Fiber-optic inter-repeater link* (lien inter-répéteur sur fibre optique). Le standard original pour l'Ethernet sur la fibre optique.
10BASE-F -- Terme générique pour la nouvelle famille d'Ethernet 10 Mbit/s : 10BASE-FL, 10BASE-FB et **10BASE-FP.** De ceux-ci, seulement 10BASE-FL est beaucoup utilisé.
10BASE-FL -- Une mise à jour du standard FOIRL.
10BASE-FB -- Prévu pour interconnecter des concentrateurs ou commutateurs au cœur du réseau, mais maintenant obsolète.
10BASE-FP -- Un réseau en étoile qui ne nécessitait aucun répéteur, mais qui n'a jamais été réalisé.
100BASE-T -- Un terme pour n'importe lequel des standards 100 Mbit/s sur paire torsadée. Inclut 100BASE-TX, 100BASE-T4 et 100BASE-T2.
100BASE-TX -- Utilise deux paires et requiert du câble CAT-5. Topologie en étoile en utilisant un concentrateur (hub) ou un commutateur (switch), comme pour le 10BASE-T, avec lequel il est compatible.
100BASE-T4 -- Permet le 100 Mbit/s (en semi-duplex seulement) sur du câble CAT-3 (qui était utilisé dans les installations 10BASE-T). Utilise les quatre paires du câble. Maintenant désuet, comme le CAT-5 est la norme actuelle.
100BASE-T2 -- Aucun produit n'existe. Supporte le mode full-duplex et utilise seulement deux paires, avec des câbles CAT-3. Il est équivalent au 100BASE-TX sur le plan des fonctionnalités, mais supporte les vieux câbles.
100BASE-FX -- Ethernet 100 Mbit/s sur fibre optique.

Gigabit Ethernet (1 000 Mbit/s)
1000BASE-T -- 1 Gbit/s sur câble de paires torsadées de catégorie 5e ou supérieure, sur une longueur maximale de 100m. Utilise les 4 paires en full duplex, chaque paire transmettant 2 bits/s par baud, à l'aide d'un code à 5 moments. Soit un total de 1 octet par top d'horloge sur l'ensemble des 4 paires, dans chaque sens. Compatible avec 100BASE-TX et 10BASE-T, avec détection automatique des Tx et Rx assurée. La topologie est ici toujours en étoile car il n'existe pas de concentrateurs 1000 Mbps. On utilise donc obligatoirement des commutateurs (switch).
1000BASE-X -- 1 Gbit/s qui utilise des interfaces modulaires (appelés GBIC) adaptées au média (Fibre Optique Multi, Mono-mode, cuivre).
1000BASE-SX -- 1 Gbit/s sur fibre optique.
1000BASE-LX -- 1 Gbit/s sur fibre optique. Optimisé pour de longues distances sur fibre monomode.
1000BASE-CX -- Une solution pour de courtes distances (jusqu'à 25 m) pour le 1 Gbit/s sur du câble de cuivre spécial. Précède 1000BASE-T et est maintenant obsolète.
Ethernet 10 gigabit par seconde
Le nouveau standard Ethernet 10 Gigabits entoure sept types de média différents pour les réseaux locaux, réseaux métropolitains et réseaux étendus. Il est actuellement spécifié par un standard supplémentaire, l'IEEE 802.3ae, et va être incorporé dans une révision future de l'IEEE 802.3.
10GBASE-CX4 (cuivre, cable infiniband, 802.3ak) -- utilise un câble en cuivre de type infiniband 4x sur une longueur maximale de 15 mètres.
10GBASE-T -- transmission sur câble catégorie 6, 6A ou 7 (802.3an), en full duplex sur 4 paires avec un nombre de moments de codage qui sera fonction de la catégorie retenue pour le câble (et de l'immunité au bruit souhaitée), sur une longueur maximale de 100 mètres. Devrait être compatible avec 1000BASE-T, 100BASE-TX et 10BASE-T
10GBASE-SR (850nm MM, 300 meter, dark fiber) -- créé pour supporter de courtes distances sur de la fibre optique multimode, il a une portée de 26 à 82 mètres, en fonction du type de câble. Il supporte aussi les distances jusqu'à 300 m sur la nouvelle fibre multimode 2000 MHz.
10GBASE-LX4 -- utilise le multiplexage par division de longueur d'onde pour supporter des distances entre 240 et 300 mètres sur fibre multimode. Supporte aussi jusqu'à 10 km avec fibre monomode.
10GBASE-LR (1310nm SM, 10km, dark fiber) et 10GBASE-ER (1550nm SM, 40km, dark fiber) -- Ces standards supportent jusqu'à 10 et 40 km respectivement, sur fibre monomode.
10GBASE-SW (850nm MM, 300 meter, SONET), 10GBASE-LW (1310nm SM, 10km, SONET) et 10GBASE-EW (1550nm SM, 40km SONET). Ces variétés utilisent le *WAN PHY*, étant conçu pour inter-opérer avec les équipements OC-192 / STM-64 SONET/SDH. Elles correspondent au niveau physique à 10GBASE-SR, 10GBASE-LR et 10GBASE-ER respectivement, et utilisent le même type de fibre, en plus de supporter les mêmes distances. (Il n'y a aucun standard *WAN PHY* correspondant au 10GBASE-LX4.)
L'Ethernet 10 Gigabits est assez récent, et il reste à voir lequel des standards va obtenir l'acceptation des compagnies.
Détails techniques de 10GBASE-R utilisé sur LAN & 10GBASE-W utilisé sur WAN et encapsulant Ethernet dans une trame SDH ou SONET.

6. La fibre optique

Bien avant l'invention du téléphone par Graham Bell (1876) , les télécommunications utilisaient déjà la voie du fil électrique (télégraphe) . Puis, grâce à Maxwell et Hertz, les informations ont emprunté la voie des airs (TSF). Finalement, dans les années 1970 est apparu le principe de la fibre optique : transmettre un signal lumineux à travers un milieu transparent.
Nous nous intéresserons donc à la fibre optique qui a connu de nombreuses avancées depuis ses débuts et en annonce de bien plus prometteuses encore : la multiplicité des paramètres, qui jouent sur l'efficacité de la fibre, fait que l'on peut sans cesse améliorer les performances de celle-ci.
On peut modifier le trajet lumineux en choisissant un type de fibre particulier, qui permettra d'obtenir un chemin optique plus court et une dispersion modale moindre.
Le signal optique subit dans la fibre des altérations tant au niveau de sa composition que de sa structure et de sa puissance, qu'il faut s'efforcer de minimiser et de compenser.
Hors de la fibre, des technologies telles que le multiplexage et les connections ou encore l'établissement d'un réseau et les techniques de codage, permettent de transmettre dans les meilleures conditions un maximum d'informations.

6.1. Le trajet lumineux et les modes de propagation

6.1.1. Historique

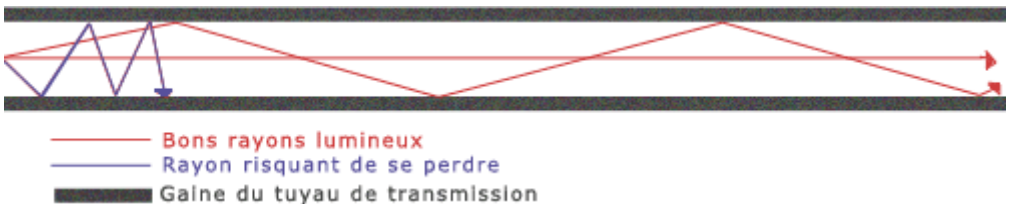
La création et les problèmes
En 1966, l'idée émerge de faire passer grâce à la lumière, les informations. Les gros problèmes de l'époque est la perte de données qui s'effectue à cause du manque de précision. Il aura fallut de nombreuses années pour la fibre optique soit à peu prés au point. Un autre problème que les premiers chercheurs ont eu du mal à résoudre c'est le fonctionnement sur de longues distances.

Aujourd'hui
Ce n'est seulement qu'avec l'amplification de la lumière dans la fibre Optique que les problèmes ont été résolus : Le laser. Ce dernier permet grâce à cette amplitude de pouvoir être diffusé sur de grandes distances. Mais aussi la concentration des particules permet une meilleure direction et maniabilité d'ou la baisse des pertes de données contre les parois du câble.

6.1.2. La lumière et la fibre optique

La lumière est donc le principal élément de la fibre optique, c'est elle qui transporte toutes les informations. Normalement, tout le monde le sait, la lumière se propage en ligne, et sans dévier, c'est pourquoi elle est conduite dans un tuyau à gaine réfléchissante, pour lui permettre de se propages quelle que soit la disposition de la fibre optique.

La lumière transportée dans la fibre optique n'arrive pas toujours au bout, elle est quelques fois malheureusement perdue. Mais plus le diamètre de la fibre sera petit, moins le risque de perte de lumière sera grand, car l'angle d'incidence de la lumière sur la gaine sera très faible (cf schéma ci-dessous), mais aussi la quantité possible de lumière transportée sera inférieure. Pour vous expliquer la réflexion de la lumière dans la fibre optique, voici un petit schéma légendé:



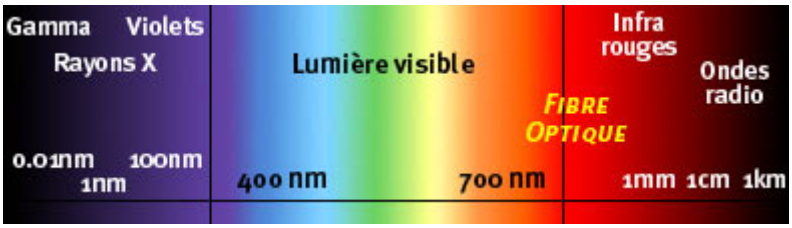
L'onde envoyée doit forcément être monochromatique (une seule couleur) pour éviter d'avoir à reconstituer les données à l'arrivée de la fibre, mais nous allons détailler cela dans le chapitre lumière.

6.1.2.1. La lumière

Il est important de rappeler dans ce chapitre tous les caractéristiques et propriétés de la Lumière pour bien comprendre le fonctionnement de la fibre Optique

6.1.2.2. Le spectre de la lumière

La lumière est une onde. En fonction de la longueur d'Onde, elle change soit de couleur soit de type (Voir Schema). L'Homme ne peut voir qu'une partie de ces ondes. Celles qui sont comprises entre 400 nanomètres et 750 nanomètres (1 nanomètre = 1 * 10^9 mètre). En dessous de 400 nm, il y a les ondes Ultraviolets, Rayons X et Gamma. Au dessus de 750 nm, il y a les rayons infrarouges. C'est, après les 750 nm, au alentour des rayons Infrarouges, que ce situe les longueurs d'Onde utilisés pour la Fibre Optique. Voici le schéma du Spectre lumineux :



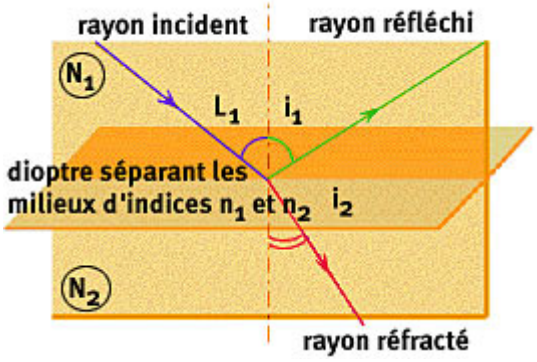
6.1.2.3. La lumière Blanche

La lumière blanche est, en vérité, le mélange de toutes les couleurs. Pour vous le démontrer, voici un schéma représentant un prisme :

La lumière blanche est donc une combinaison de toutes couleurs. Ce sont leurs différentes longueurs d'Ondes qui nous permettent de visualiser avec un prisme toutes les couleurs. Etant donne que l'indice du milieu n2 varie très légèrement en fonction de la longueur d'Onde. Donc l'angle de réfraction est d'abord modifier par le premier coté du Prisme puis est encore amplifié par le second coté heurté par les longueurs d'Onde couleurs. D'ou la palette de couleurs à la sortie du Prisme

6.2. La Réfraction et la réflexion

Un élément important : Cela dépend du milieu.
Si les deux milieux (d'incidence et d'impacte) sont Homogènes et transparents (voir schéma) :
D'après le lois de Descartes-Snell, le milieu ou se trouve la lumière avant l'impacte est appelé 1 et possède un indice n1 qui dépend de nombreux critères. Le milieu d'impacte sera appelé 2 avec un indice n2. Lorsque la lumière heurte le milieu 2, elle va changer de direction. Son angle d'incidence (i1 en radian) va décider de sa direction. Si n1 * sin(i1) <1 alors il y a réfraction: car l'équation n1 * sin(i1) = n2 * sin(i2). Lors d'une réfraction la lumière traverse le milieu 2 avec un angle i2. Si n1 sin(i1) >1 alors la lumière est réfléchit en un angle identique à i1. Voici un schéma permetant de mieux visualisés les lois de la réflexion et réfraction :



Si le milieu de départ est plus dense que le milieu d'impacte, alors il existe plus un angle de réflexion. L'angle entre la réfraction et la réflexion est appelé angle critique. Grâce à cela, la lumière peut circuler indéfiniment dans un câble de verre. Plus le diamètre du câble sera faible plus l'angle critique ne pourra être atteindre.

6.3. La vitesse de la lumière

La vitesse de la lumière varie légèrement en fonction du milieu auquel il se situe. Mais elle atteint environ les 300000 Km/s : Ce qui est la vitesse la plus importante connu à ce jour.

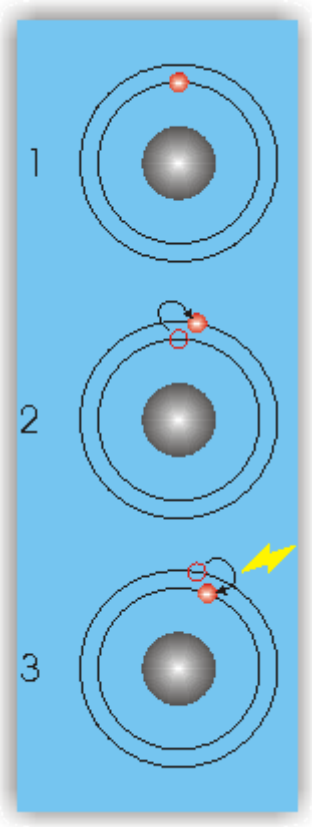
6.4. Le Laser

Nous allons dans ce chapitre expliquer le principe et le fonctionnement d'un laser puisque la fibre Optique a pour obligation de l'utiliser.

6.4.1. Définition

Laser, en anglais Light Amplification by Stimulated Emission of Radiation ou en français Amplification de la lumière par émission de radiation stimulé, est une émission de lumière par ondes lumineuses avec la même phase, permettant par exemple la fabrication d'un faisceau très concentré (allant jusqu'au découpage de matériaux). Le laser permet une précision extrêmement plus importante que les autres faisceaux lumineux. Le laser est utilisé par la Fibre Optique pour amplifier le rayon lumineux et ainsi réduire les pertes de la Fibre Optique.

6.4.2. La Création de la Lumière



La création de la lumière est effectuée par un surplus d'énergie au niveau de l'atome. Un Atome possède un noyau, composé de protons et de neutrons, et autour du noyau circule des électrons. Les électrons gravitent sur "plusieurs niveaux", appelés couches. Ils ont une place bien déterminée dans les couches. Seul un surplus d'énergie sur les électrons les fait montés de couches. L'électron doit se replacer et pour cela rejette de l'énergie sous forme de photons : c'est la lumière. Voici un schema détaillant ce processus :

6.4.3. Fonctionnement d'un laser

Le principe du laser est de produire des photons totalement identiques. Pour cela, on utilise un gaz tel qu'hélium-neon ou un rubis ou une source d'électricité. On utilise un tube, fermé d'un coté par un miroir totalement réfléchissant et composé de l'autre coté d'un miroir semi transparent c'est à dire ne réfléchissant qu'une partie. On place dans le tube des atomes très précis (ex: rubis). Les atomes sont excités par une source d'énergie (tel que l'électricité) d'ou une création de photons. Cette création de photon se réfléchisse sur les miroirs et percute les atomes, créant ainsi le passage des électrons à une couche inférieure. Les électrons doivent alors former des photons d'énergie identique à celui qui les a percutés. Une nouvelle formation de photon identique à l'initial se propage dans le tube. Ainsi de suite. Certains photons passent le miroir transparent : c'est l'émission d'un faisceau laser.

6.4.3.4. Utilisation d'un laser

Le laser est utilisé pour la lecture de CD, le soudage, le découpage, la gravure ou le plus important la fibre Optique. Les scientifiques cherchent à mettre au point des lasers à ondes lumineuses très courtes.

6.5. Fibre multimode à saut d'indice

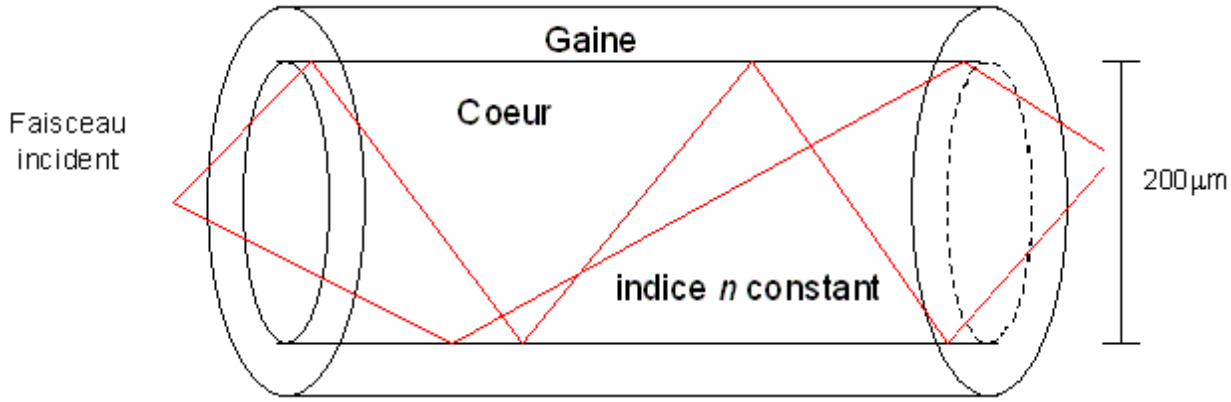


Figure : La fibre à saut d'indice

Les fibres à saut d'indice présentent un cœur transparent d'indice constant, et une gaine sombre, il y a alors réflexion du rayon lumineux à la frontière entre les deux matériaux. Cependant, le chemin optique varie, ce qui est gênant puisqu'un même signal se retrouve étendu à la sortie.

6.6. Fibre multimode à gradient d'indice

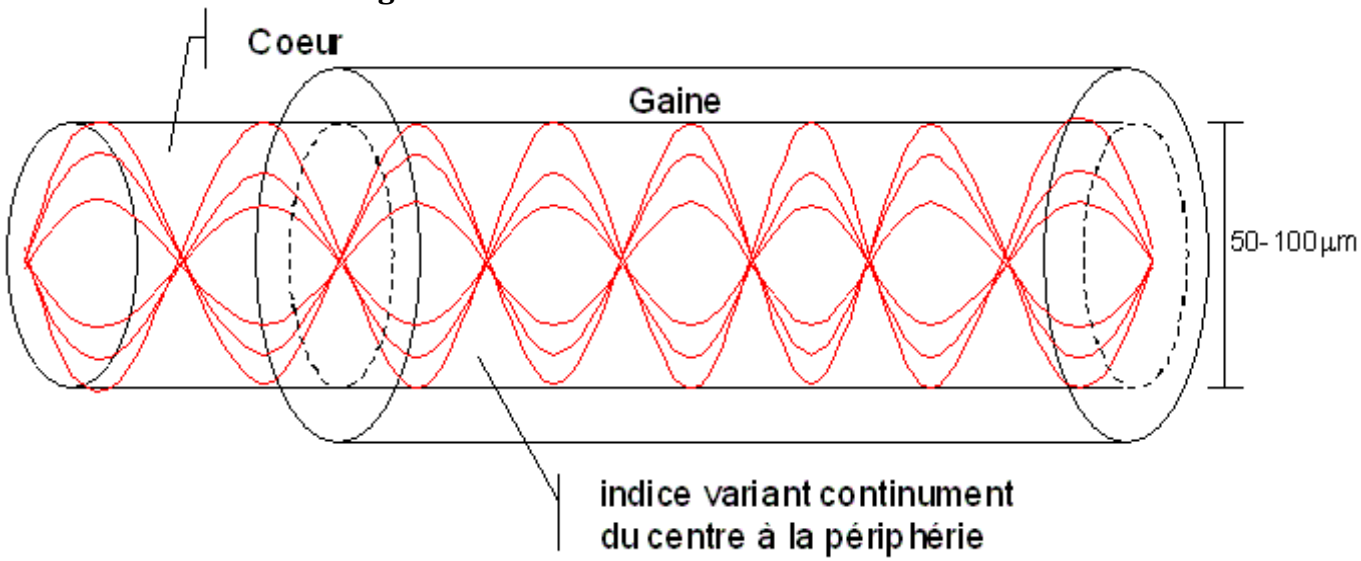


Figure : La fibre à gradient d'indice

Ici l'indice varie peu à peu du centre à la gaine, la forme de la trajectoire est plus sinusoïdale car le rayon est dévié au fur et à mesure qu'il s'éloigne du centre.

La variation de chemin optique est ici plus faible car le coeur a un diamètre moindre.

L'étalement du signal est moins important grâce à la variation de l'indice.

6.7. Fibre monomode

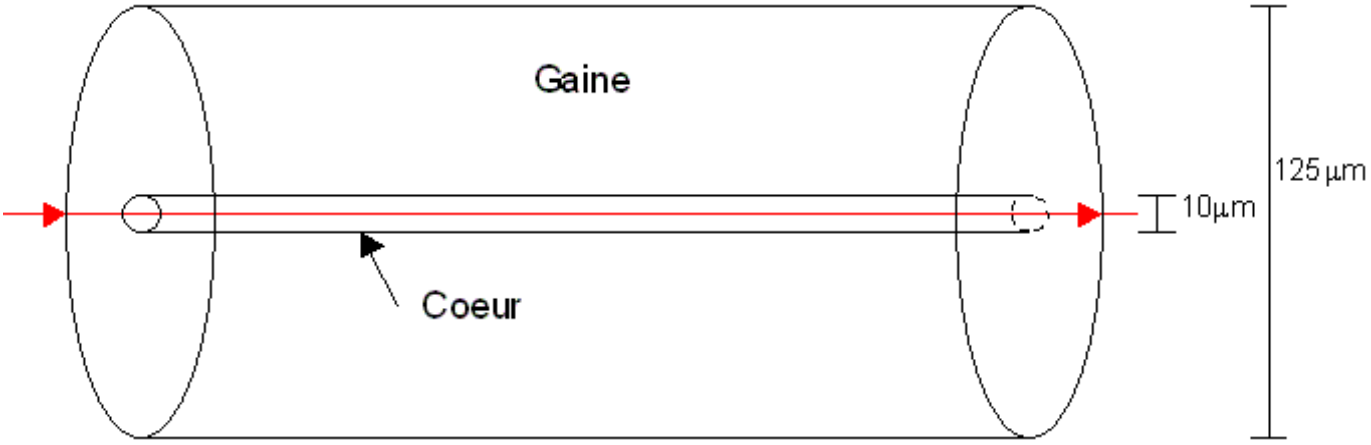


Figure : La fibre monomode

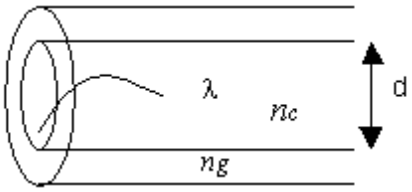
Dans une fibre monomode, on obtient un seul mode grâce à la très faible dimension du cœur (diamètre de 10 mm et moins) . Ainsi le chemin de la lumière est imposé, il n'y en a qu'un seul : celui du cœur . Il existe expérimentalement des fibres optiques monomodes à cristal photonique.

6.8. Modes et dispersion modale

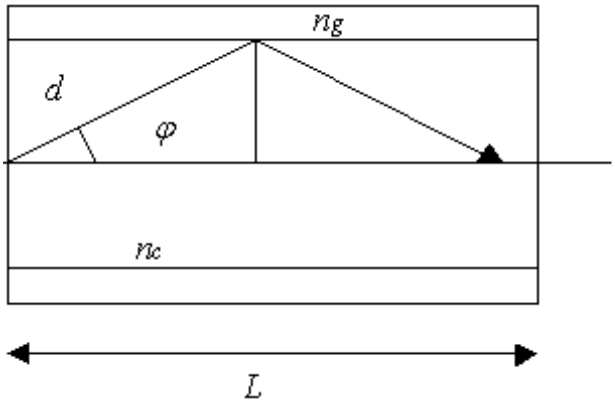
Les modes sont l'expression des différents chemins optiques que peut suivre le signal dans la fibre.
Une formule expérimentale donne le nombre de modes dans une fibre à saut d'indice :

$$N \approx \left(\frac{2\pi}{\lambda} d \sqrt{n_c^{\,2} - n_g^{\,2}} \right)^2$$

$$avec \ \sqrt{n_c^{\,2} - n_g^{\,2}} \ l'ouverture\ numérique$$



L'ouverture numérique traduit l'angle d'entrée des faisceaux lumineux dans la fibre.
On voit que le nombre de modes dépend du diamètre du coeur au carré ! Il est donc important de minimiser le diamètre du cœur. La valeur des indices et la longueur d'onde choisie influent, mais dans une moindre mesure.
Expliquons la dispersion modale :



$$d = \frac{L}{\cos\varphi},$$

$$\tau = \frac{n_c}{C}\frac{L}{\cos\varphi}, \ C \text{ la vitesse de la lumière}$$

τ le temps de parcours

Le plus court chemin est sur l'axe optique :

$$\tau_{min} = \frac{n_c}{C}\frac{L}{\cos\varphi} = \frac{n_c \cdot L}{C}$$

Le plus long est réalisé pour l'angle limite au-delà duquel il n'y a plus réflexion :

$$\tau_{max} = \frac{n_c}{C}\frac{L}{\cos\varphi_{lim}} où \cos\varphi_{lim} = \frac{n_g}{n_c}$$

$$\Delta\tau = \tau_{max} - \tau_{min} = \frac{{n_c}^2 \cdot L}{C \cdot n_g} - \frac{n_c \cdot L}{C} = \frac{n_c \cdot L}{C}\left(\frac{n_c}{n_g} - 1\right)$$

$$\text{ainsi} : \Delta\tau = \frac{n_c \cdot L}{C}\left(\frac{n_c - n_g}{n_g}\right) = \frac{\Delta n \cdot L}{C}\frac{n_c}{n_g}$$

$$\Delta\tau \approx \frac{\Delta n \cdot L}{C}, avec \frac{n_c}{n_g} \approx 1, car, \Delta n = n_c - n_g << n_c, n_g$$

Pour *L*=1 km, n_c=1.43 , n_g=1.42 , Dt=33 ns , ce qui n'est pas négligeable . On voit que déjà sur 1 km , la dispersion modale introduit un retard notable , c'est pourquoi les fibres multimodes ne sont utilisées que pour des réseaux locaux .

6.9. Le signal optique

6.9.1. La dispersion chromatique

Lorsque l'on envoie un signal lumineux, il y a plusieurs longueurs d'onde présentes , soit parce que la source est étendue , soit parce que la source présente en réalité un pic centré sur l .
Par exemple, une LED (light emitting diode), a un pic d'une largeur de 10 nm, un laser, un pic d'une largeur d'1 nm et moins.

Le mode fondamental a une constante de propagation définie par $\beta = \frac{2\pi}{\lambda} n_c$. Le temps de propagation est : $\tau = \frac{L}{C} \cdot n_c = L\left(\frac{\partial\beta}{\partial\omega}\right)$ avec $\omega = 2\pi\frac{C}{\lambda}$. La dispersion chromatique traduit les variations de t selon l : $\boxed{D = \frac{1}{L}\frac{\partial\tau}{\partial\lambda}}$. La dispersion a deux composantes : la dispersion due au guide et aux variations d'indice, et la dispersion due à la longueur d'onde.

On a : $\frac{\partial\tau}{\partial\omega} = L \cdot \frac{\partial^2\beta}{\partial\omega^2}$, on écrit alors : $\boxed{\Delta\tau = \beta'' \cdot L \cdot \Delta\omega}$

On voit que la différence de temps de parcours d'un signal de largeur spectrale Dw, dépend de celle-ci , de la longueur *L* de fibre parcourue et de b '' , dérivée seconde de la constante de propagation du mode .

On a : $D = \frac{1}{L}\frac{\partial\tau}{\partial\omega}\frac{\partial\omega}{\partial\lambda}$, avec $\frac{\partial\tau}{\partial\omega} = \beta'' \cdot L$ et $\frac{\partial\omega}{\partial\lambda} = 2\pi \cdot C\frac{\partial\frac{1}{\lambda}}{\lambda} = -\frac{2\pi \cdot C}{\lambda^2}$

D'où : $D = -\frac{2\pi \cdot C \cdot \beta''}{\lambda^2}$ et $\beta'' = \frac{-D}{\frac{2\pi \cdot C}{\lambda^2}}$ avec $\Delta\tau = \beta'' \cdot L \cdot \Delta\omega = D \cdot L\left(\frac{-1}{\frac{2\pi \cdot C}{\lambda^2}}\right)\Delta\omega$

Comme $\omega = 2\pi\frac{C}{\lambda}$, $\Delta\omega = \frac{-2\pi \cdot C}{\lambda^2}\Delta\lambda$, d'où $\boxed{\Delta\tau = D \cdot L \cdot \Delta\lambda}$

Pour corriger la dispersion chromatique, on fait appel à un réseau de Bragg à pas variable.

Un réseau de Bragg à pas constant se comporte comme un filtre pour une longueur d'onde donnée. Avec un réseau à pas variable, on travaille sur toute une bande spectrale, on ralentit les longueurs d'onde les plus rapides . En optimisant la variation continue du pas du réseau, le signal issu de ce réseau retrouve sa forme d'origine.

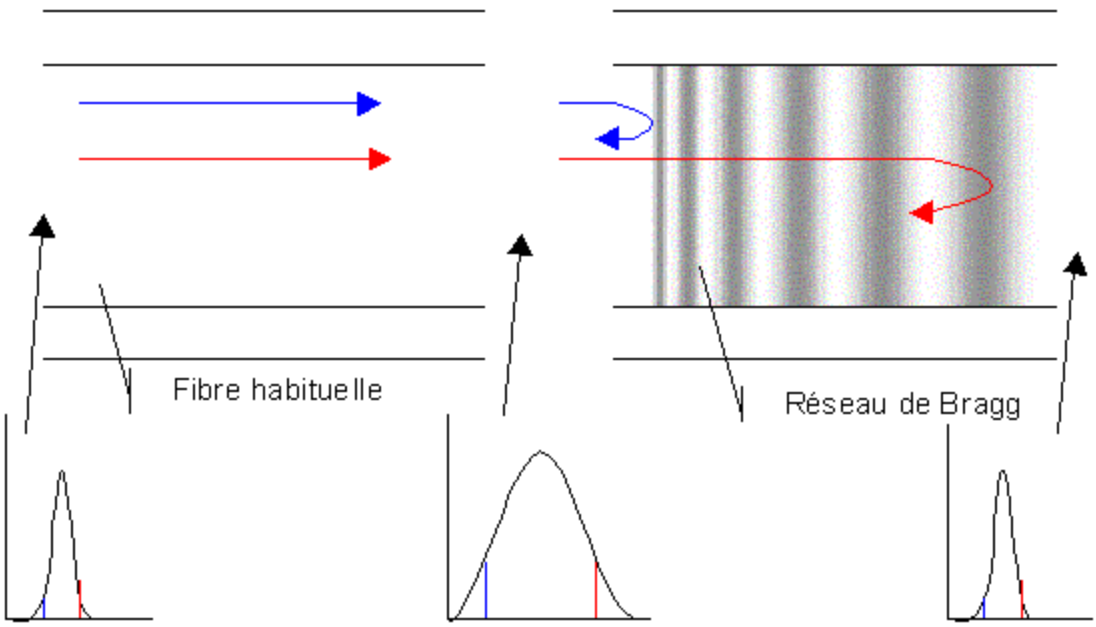


Figure : Effet sur un signal d'une fibre à réseau de Bragg à pas variable

Un réseau de Bragg est inscrit dans la fibre par holographie ou bien par chauffage, tension ou pression, sur un segment de quelques centimètres.

D'après Optics Letter, la méthode par compression (avec une compression de 2.7 % est plus efficace que la tension, mais il y a une force limite à ne pas dépasser pour ne pas rompre la fibre : environ 22 Newton. Par contrôle actif, on obtient un réseau à variations continues et un gain identique pour toutes les longueurs d'onde.

6.9.2. La dispersion de polarisation

Dans l'absolu, on ne réalise pas de fibre parfaite ; le problème auquel nous nous intéressons ici est la polarisation de la lumière dans la fibre.

Les imperfections de fabrication produisent un coeur de forme plutôt elliptique. De plus, à l'utilisation, les courbures déforment aussi la fibre ; on a alors un milieu anisotrope : au vu du faisceau, il y a des indices différents selon la direction. Dans la fibre, on constate une biréfringence : un rayon non polarisé incident est décomposé en deux rayons (extraordinaire et ordinaire) polarisés linéairement mais l'un en mode transverse magnétique [TM] et l'autre en mode transverse électrique [TE].

Plusieurs corrections existent :

- Un système électrique peut, de loin en loin sur la fibre, capter le signal et après analyse émettre le signal comme à son origine. On perd ici l'efficacité du traitement tout optique.
- Des fibres à maintien de polarisation comme les fibres à coeur elliptique ou les fibres PANDA ou TIGER.

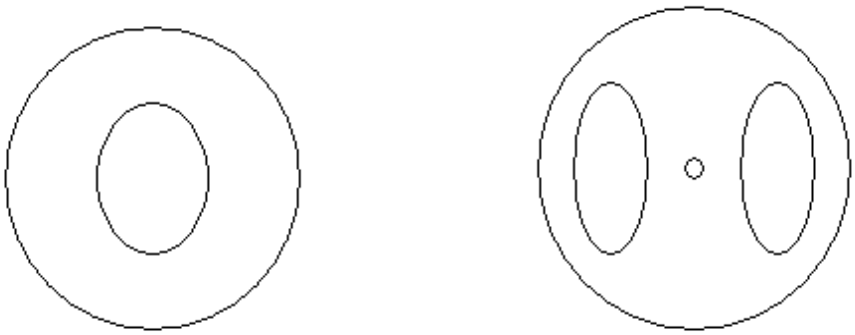


Figure : Fibres à maintien de polarisation

Avec ces fibres, on peut contrôler la polarisation le long de la fibre.

La perte de polarisation est utile (eh oui !) pour l'utilisation des fibres comme capteurs : lorsque la fibre subit des contraintes, le signal est modifié et on peut l'analyser.

L'atténuation

Dans une fibre optique réelle on constate que toute l'énergie lumineuse entrante n'est pas récupérée en sortie. Il y a des phénomènes de dispersion causes de cette perte (ou atténuation) qui dans une fibre de télécommunication, pour une longueur d'onde optimale de 1550nm, atteint environ 0.17dB/km contre 2.5db/km à 850nm et 0.3db/km pour 1300nm.

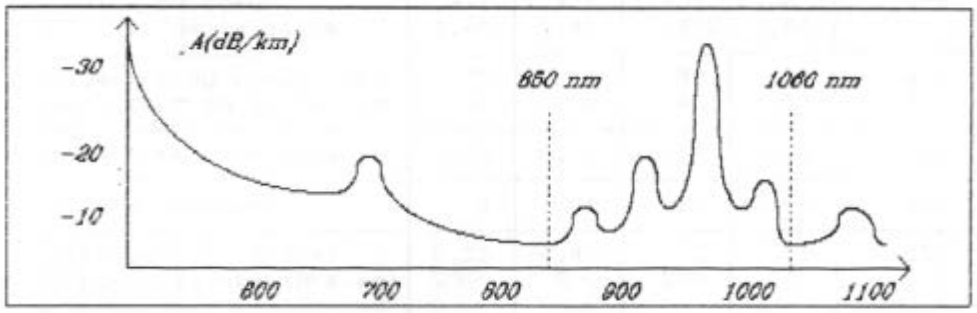


fig. courbe d'atténuation d'une fibre QSF A 200 (doc. Quartz et Silice)

Les causes des pertes dans les fibres sont multiples. On distingue généralement :

L'absorption par les impuretés, en effet une fibre de silice quoique très purifiée n'est pas parfaite et les atomes d'impuretés vont avoir plusieurs effets perturbateurs dont l'absorption purement et simplement du photon par un électron de l'atome avec transformation finale de l'énergie lumineuse du photon en chaleur

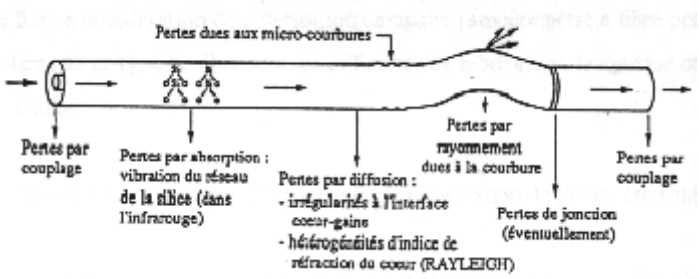
La diffusion par les impuretés ou par les défauts d'interface cœur gaine et la diffusion Rayleigh qui est la diffusion de la lumière sur les molécules du matériau (la silice), due à des variations locales de l'indice de réfraction créées par des changements de densité ou de composition apparus au moment de la solidification du matériau

La dispersion chromatique due aux vitesses différentes de signaux lumineux de longueurs d'onde différentes

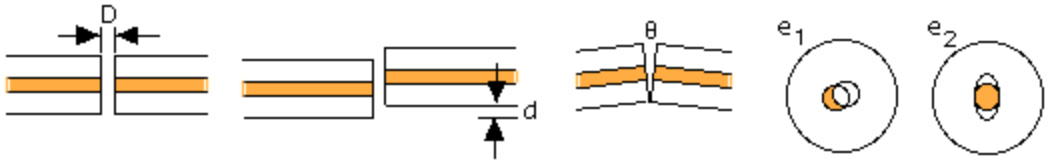
La dispersion intermodale résultant des temps de propagation différents selon les modes

Les courbures et les micro courbures de la fibre, la fibre ne peut pas dans une application réelle être, sauf exception, exempte de courbures et dans ces zones le risque pour un rayon lumineux de ne plus satisfaire la condition de réflexion totale est inévitable ce qui se traduit par une perte dans la gaine par simple réfraction.

La diffusion et la réflexion aux épissures,



Nous nous intéresserons plus particulièrement à ce problème de connectique. C'est actuellement l'une des sources les plus importantes des pertes d'une ligne de fibre optique unimodale. En effet lors d'une connexion bout à bout on peut avoir :
Une séparation longitudinale,
Un désalignement radial,
Un désalignement angulaire,
Une excentricité des coeurs,
Voire une ellipticité des coeurs.



La connexion entre deux fibres semblables s'effectue de deux manières : Dans une première technique on réalise une épissure à l'aide d'une machine spécialisée (une épissure) réalisant une véritable soudure entre les deux fibres mises bout à bout par fusion au micro chalumeau ou plus fréquemment à l'aide d'un arc électrique. Le positionnement relatif des deux fibres est réalisé grâce à des micromanipulateurs et contrôlé optiquement. Typiquement en envoyant un faisceau intense dans l'une des fibres et en mesurant la quantité de lumière transmise dans l'autre. Le positionnement idéal coïncide évidemment avec une maximum de lumière transmise. Notons que réaliser une épissure en laboratoire est relativement aisé, mais le gros problème est de réaliser une épissure sur site. Pour résoudre ce problème de nombreux constructeurs ont réalisé de véritables connecteurs tels ceux figurés ci-dessous.

6.9.3. Les applications de la fibre optique

De nos jours, les stations de travail sont connectées entre elles a l'aide de réseaux utilisant la fibre optique car son utilisation permet des débits d'informations plus rapides et une plus grande sûreté lors des transmissions. En téléphonie, les câbles coaxiaux sont remplacés peu à peu par des fibres optiques en effet, elle est plus économique sur longues et courtes distances et le nombre de composants nécessaires est moins important. Son utilisation est particulièrement intéressante pour les militaires car elle leur apporte certains avantages:
-faible poids
-taille de la fibre
-insensibilité au brouillage et à la détection

6.9.4. La fibre optique en France

6.9.4.1. La technique de télédistribution

La fibre optique a été retenue pour ces liaisons car, sur des distances relativement longues, son affaiblissement faible évite la pose de répéteurs, à la différence du coaxial et des liaisons hertziennes qui n'auraient pas été interactives. France-télécom se charge de la réception des programmes puis les transmet vers la régie de l'opérateur. Ils sont ensuite acheminés par fibre optique vers le centre de supervision France-Télécom puis vers les centres de distribution.
Le premier réseau urbain en fibre date de 1980 à Paris, entre deux centraux électroniques. Les premières commandes de série ont été passées en 1982 et le début des réalisations massives remonte à 1983. Depuis 1987 est utilisée la nouvelle fibre monomode. Actuellement trois quarts des fibres sont installés en région parisienne entre des centraux téléphoniques. Elles fonctionnent sans répéteur à 34 Mbits/s. Fin 1988 150000 Km de fibre était en service et 300 000 km commandés.
Environ 200 000 km de fibre seront posés en interurbain d'ici 10 ans. En 1989 30000 km de fibres seront posées. Des liaisons optiques relient Paris à Strasbourg, Lyon, Nantes, Lille d'une part et Lyon Marseille d'autre part.
La stratégie de la direction générale des réseaux nationaux est la suivante:
Passer à la fibre pour tous les axes importants risquant la saturation à court et moyen terme.
Rechercher la connexité optique.
Viser la desserte optique des grandes villes.

Les simulations sont favorables malgré les travaux de génie civil nécessaires. Des économies se feront sur l'extension des systèmes traditionnels et la mise hors service des vieux coaxiaux chers à entretenir. On ne pose plus de coaxial.
En 1987, la fibre était 2 à 3 fois moins chère que le coaxial pour la fabrication et aussi pour l'équipement des systèmes. Elle sera utilisée pour le transfert des données numériques entre les centres de transit interurbains où on l'installe progressivement en remplacement du coaxial. Une partie des réseaux fibre optique urbains utilisés actuellement pour la télédistribution sert occasionnellement en dépannage pour les liaisons téléphoniques et le transfert de données.
Mais la fibre optique est déjà directement à la disposition des entreprises, dans plusieurs configurations:

6.9.4.2. Les zones de télécommunications avancées (ZTA)

En Janvier 1989 a été inaugurée la première zone de télécommunication avancées de France sur le technopole de Metz-2000. Des services très performants de télécommunications sont offerts aux offerts aux entreprises : réseaux fibre optique rattachés au RNIS 2ème génération, possibilité de raisons par les satellites Telecom 1 et IBS aux métropoles américaines et européennes.

6.9.4.3. Vidéodyn

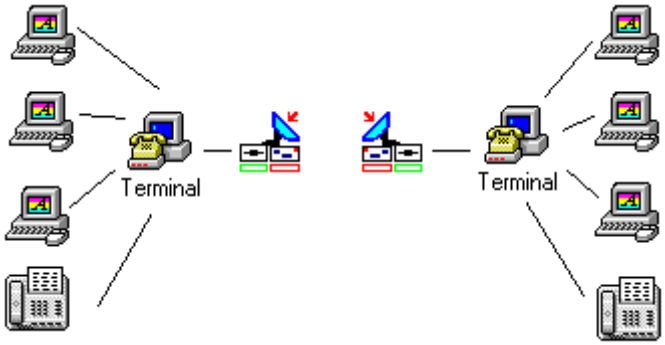
Ce nom rassemble l'ensemble des moyens mis à la disposition des clients soit abonnés soit occasionnels pour les transmissions télévisuelles. Les réseaux urbains d'acheminement utilisent pour partie la fibre optique dans les grandes villes : ils assurent les liaisons entre les centraux téléphoniques et alimentent les centres de distribution des quartiers. En plus des images destinées au grand public, ces matériels sont capables de transporter, sur des fibres, des signaux haut débit à large bande pouvant être utilisés pour établir des liaisons permanentes ou temporaires entre différents équipements.

6.9.4.4. Le RNIS large bande

Le RNIS se base sur une structure complètement numérique et optique. Des concentrateurs satellites numériques raccordent les téléphones analogiques et numériques aux commutateurs numériques. Le RNIS est mis en place depuis 1987 dans les côtes du nord. Il l'est maintenant sur Paris et dans toute la France.Les raccordements numériques normalisés adaptés au volume de communication de chaque usager permettent le transport de la voix, de la télécopie, du vidéotex et des données jusqu'à deux fois 64Kbits/s sur un câble unique. Les services sur réseaux fibre optique à large bande compléteront donc ceux de la première génération à bande étroite : les banques multimédias permettront la vidéothèque, le téléchargement de vidéocassettes ou de logiciels.

6.9.4.5. La domotique

La gestion technique centralisée d'un bâtiment intelligent peut comprendre la détection incendie, les inondations, les fuites de gaz, alerte des services compétents, télésurveillance etc... Cela nécessite un "bus domestique" à base de fibre optique.

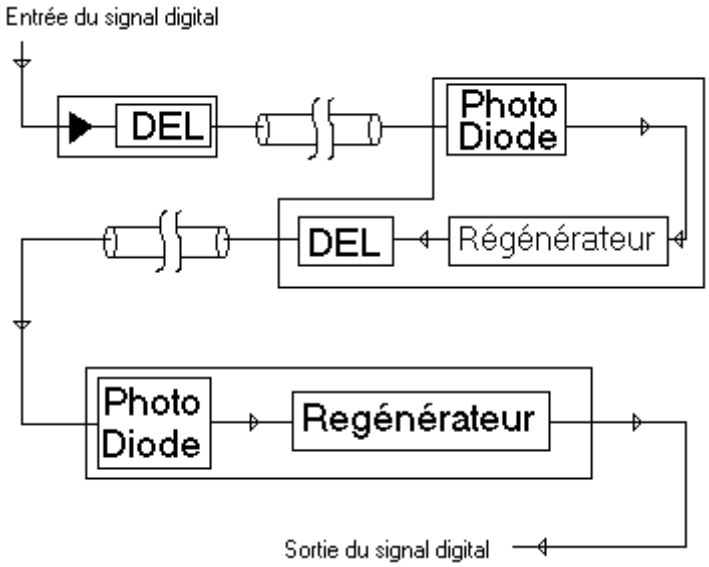


6.9.5. Les transmissions numériques par fibre optique.

6.9.5.1. Le transfert d'informations

L'émission consiste à coder l'information, c'est à dire moduler le porteur d'information, qui est ici le faisceau lumineux.
La réception quant à elle consiste à décoder et à interpréter les signaux émis.
Le débit d'information est limité par entre autres, la dispersion du matériau, et par la variation des différentes vitesses. (La dispersion du matériau est liée à la nature du milieu, car l'indice du corps constituant la fibre varie en fonction de la longueur d'onde).C'est le nombre de modes qui est à l'origine de ce problème. Celui-ci dépend du rayon de la fibre, et des indices des différents milieux qui la constituent.
Le débit maximal d'informations est donc limité par le nombre de modes, car ceux-ci entraînent une déformation du signal.
Il est possible de montrer que le débit maximal d'informations est :
Avec :
- L : la longueur de guide.
- h '' : la dérivée seconde du vecteur d'onde du guide par rapport à la fréquence.
- d : fraction de puissance de recouvrement permise entre deux impulsions consécutives.

On peut par exemple moduler le signal de la façon suivante :
L'émetteur envoie un train d'impulsions périodiques, (onde porteuse). L'information binaire est le signal à envoyer. La modulation peut se schématiser par le produit dans le temps deux fonctions, et le train d'onde initial se trouve amputé d'un certain nombre d'impulsions.



6.9.5.2. Transmission optique

Les transmissions numériques par fibre optique constituent l'essentiel des liaisons en fibre optique. En effet, la médiocrité des composants optoélectroniques se prête mal aux transmissions multiplexées analogiques. (Bien que certaines applications existent dans le domaine de la vidéo et des mesures.)
D'autre part, la faible atténuation et la grande bande passante permettent de tirer tout le parti des transmissions numériques.
Dans les grandes lignes, on retrouve l'organisation d'une liaison numérique sur câble, cependant, la faible atténuation de la fibre liée au faible rapport signal/bruit exigé en numérique permet des pas de régénération de plusieurs dizaines de kilomètres. Cela permet de concevoir des nombreuses liaisons sans répéteur, ou du moins avec alimentation locale.

6.9.5.2.1. Description des équipements :

- Emission et réception, par l'intermédiaire d'interfaces optoélectroniques d'émission (IOE) et de réception (IOR), ce dernier étant suivi d'une régénération du signal numérique, avec récupération de l'horloge en ligne.
  Ces fonctions sont également présentes dans les répéteurs.

- Transcodage, pour passer du code à la jonction au code en ligne. Cette opération permet la récupération du rythme quel que soit le message numérique, et éliminent les composantes continues et trop basse fréquence. Elle permet la mesure du taux d'erreur moyen par comptage des manquements observés à la règle de codage (mais non la localisation et la correction.). Le transcodage en télécommunication optique est unipolaire à deux niveaux (e type tout ou rien). On utilise principalement :
    - Le code biphase pour les transmissions de données :

  0 est codé par 01
  1 est codé par 10
    - Le code CMI, jusqu'à 34 Mbits/s :

  0 est codé par 10
  1 est codé alternativement par 00 et 11
    - Les codes de blocs binaires type nBmB au-delà :

  Un bloc de n bits est traduit par un bloc de m bits. (Les plus courants sont 3B4B, 5B6B, 7B8B). Ces codes sont plus complexes, mais le débit en ligne est multiplié par m/n, au lieu de 2 en CMI.
- Surveillance du bon fonctionnement de la liaison :
  Présence du signal en émission et en réception,
  Présence de l'horloge en émission et en réception,
  Bon fonctionnement des interfaces optoélectroniques.
  Taux d'erreurs excessif.
- Télésurveillance :

des répéteurs par réception des messages qu'envoient leurs systèmes de surveillance, et commandes éventuelles d'une correction,
télélocalisation (par bouclages successifs) d'une section de câbles en défaut ou coupée.

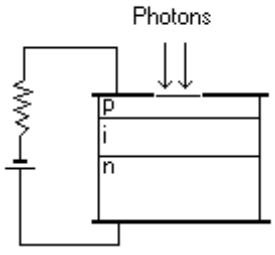
6.9.5.2.2. Emission

On utilise des diodes électroluminescentes, qui ont un fonctionnement impulsionnel, ou des diodes laser, dont l'intensité est modulée en fonction de l'information.

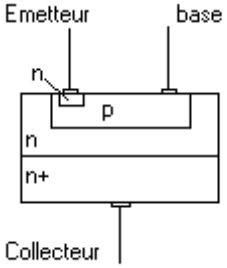
6.9.5.2.3. Réception

On utilise soit une photodiode, qui module le courant en fonction de l'information reçue, soit un phototransistor. Il faut obligatoirement associer un préamplificateur à la photodiode, alors que pour le transistor, le photocourant est amplifié par le gain en courant.

Une photodiode :



Un phototransistor :



6.9.5.3. Les problèmes de transmission

6.9.5.3.1. Les différents types de pertes

Bien que très performantes les fibres optiques subissent des atténuations lors de la propagation du signal.
L'atténuation se mesure en db/km et elle dépend de la longueur d'onde.
Elle est due à plusieurs phénomènes :

- **La diffusion Rayleigh**

Elle est due à l'interaction entre la lumière et la matière. En effet des milieux comme le verre, les liquides et les gaz diffuse la lumière. Cette diffusion est d'autant plus grande que la longueur d'onde est petite, d'où l'utilisation de l'infrarouge (longueur d'onde élevée).

- **Absorption**
  - due à la présence d'impuretés dans la fibre par exemple les liaisons OH
  - transition électronique dans l'ultraviolet
  - vibration moléculaire
- **Dispersion nodale et bande passante**

Lors de la propagation de la lumière, une même impulsion peut se propager par plusieurs chemins à la fois. Du coup, une impulsion émise très brève (pic étroit) sera reçue sur un temps plus long (tache plus large): c'est la dispersion nodale.
Plus la largeur des pic de réception est grande moins on peut rapprocher des impulsions dans le temps sinon il y a risque de chevauchement à la réception.
Donc plus les images sont étroits plus la bande passante est grande et plus la vitesse de transmission est rapide.

- **Raccordements**

Il y a 2 manières de mettre bout à bout 2 fibres, par épissure (fusion) c'est un raccord définitif ou par connecteur pour les raccords démontables.

Dans les deux cas (surtout le 2éme), cela entraîne des pertes à cause :

- de l'écartement
- de l'excentrement
- du désalignement

- **Courbure et microcourbure**

Avec une courbure il y a diminution de l'angle entre le rayon et la normale à la fibre. Pour une propagation il faut que le rayon soit réfléchi mais au-dessus d'angle le rayon est réfracté par la gaine optique.
La courbure est due à une déformation globale de l'axe.
La microcourbure est due à une déformation locale de l'axe l'effet est le même.

6.9.5.3.2. Solution pour compenser les pertes : l'amplification

Pour compenser toutes ces pertes, notamment sur longue distance on est obligé d'insérer des amplificateurs. Par exemple pour les liaisons à travers l'atlantique il faut en mettre tout le 150 km. Cette distance varie suivant le type de fibre utilisée.
Le principe est simple, on associe un récepteur puis un amplificateur électrique puis un émetteur.
Ce procédé permet donc de renvoyer un rayon d'intensité plus forte mais aussi de recréer des images d'impulsions plus étroites. Mais il nécessite une alimentation électrique. Pour cela de nombreux câbles optiques sont gainés avec du cuivre, ce qui augmente la solidité et permet le passage du courant.

6.9.5.3.3. Technologies environnantes

6.9.5.3.3.1. Le multiplexage WDM et DWDM

A l'heure actuelle, le besoin en bande passante est une réalité effective. Mais poser une fibre a un coût non négligeable et on ne peut pas se permettre de poser plusieurs fibres pour augmenter la quantité d'informations transportables. Il est donc nécessaire de faire en sorte d'exploiter au maximum les fibres existantes déjà installées. D'où l'idée du multiplexage : transmettre plusieurs signaux simultanément dans la même fibre.
Le Wavelength Division Multiplexing (WDM) et le DenseWDM (DWDM) sont des technologies permettant de transmettre plusieurs signaux simultanément dans une même fibre optique. On cherche dans tous les cas à optimiser l'utilisation de la fenêtre de transmission de la fibre (environ 100nm). (Il existe aussi le CoarseWDM qui est une autre norme).
Le WDM sépare chaque canal de 0.8nm et le DenseWDM de 0.2nm.
L'intérêt de la fibre optique est que ces signaux ne peuvent se confondre, à la réception ils seront parfaitement distingués.

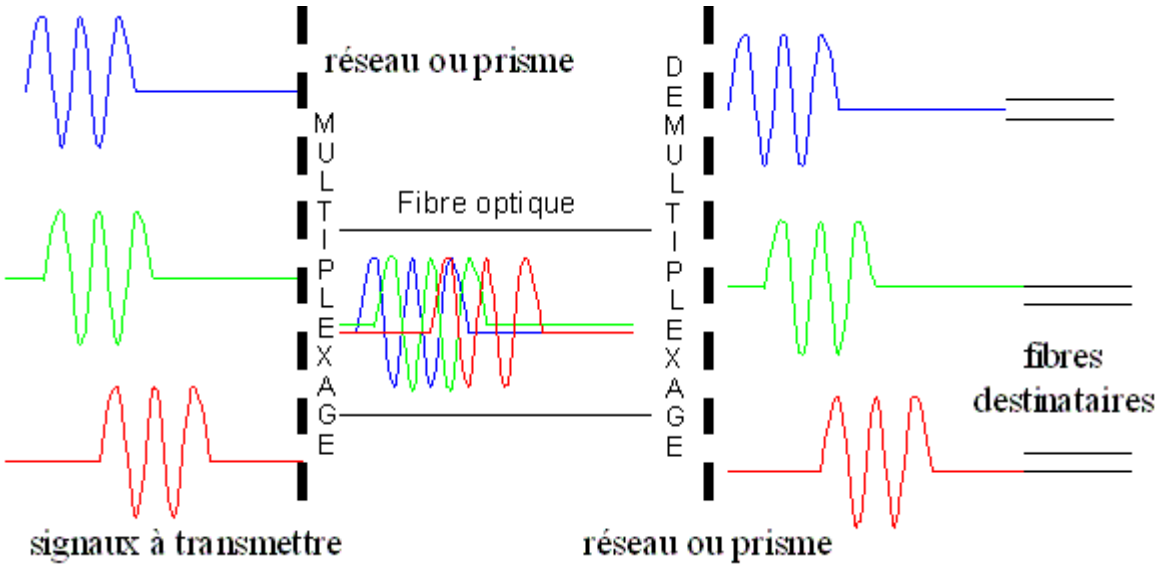


Figure : Principe du multiplexage

On réalise le multiplexage principalement dans des fibres monomodes.

A partir de plusieurs lasers à spectre fin ou d'un seul à spectre large, on réalise un échantillonnage de longueurs d'onde de l'ordre du 1/10 ème de nanomètre.

On parvient à l'heure actuelle à réaliser 256 canaux dans une seule fibre.

Un système que l'on appelle OADM (Optical Add Drop Multiplexer), permet d'inclure un canal supplémentaire ou d'en retirer un à un lieu précis de la fibre , ceci se réalise à l'aide de filtres (comme des réseaux de Bragg par exemple) .

En réalisant un échantillonnage de plus en plus fin, on pourra obtenir des fibres à très large bande passante, et ajouté au système OADM (avec le principe d'une autoroute : on peut aller d'un bout à l'autre ou sortir - rentrer en un lieu précis) cela permettra d'obtenir un réseau flexible. Le multiplexage est ainsi une technologie incontournable des télécommunications par fibre optique.

6.9.5.3.3.2. Un réseau optique

La principale application de la fibre optique se trouve dans les télécoms ; on construit donc des réseaux à l'échelle d'une entreprise, d'une ville, d'une région, d'un pays et même au-delà (câbles transatlantiques) .

A l'échelle d'un pays, un réseau comporte ce que l'on appelle une épine dorsale (en anglais backbone) assurée par une fibre à très haut débit , qui dessert des réseaux plus locaux sur toute sa longueur ; une telle ligne ne boucle pas , c'est ce que l'on appelle pour un réseau , une topologie point à point . De telles fibres parcourent plusieurs centaines de kilomètres et requièrent un certain nombre d'amplificateurs, qu'il faut minimiser car ils augmentent le coût du réseau. On installe sur ces lignes des OADM qui permettent de délivrer un canal précis à un réseau local.

L'autre forme de réseau correspond à une plus petite échelle : ce sont les LAN et les MAN (Local et Metropolitan Area Networks). Ils prennent, eux, une topologie en anneau, en maille de filet, ou en étoile, pour assurer les communications et échanges de données à l'échelle locale (entreprises, particuliers). Ces réseaux, ont pour centre névralgique un hub qui rassemble les fonctions de multiplexage - démultiplexage, d'amplificateur, de commutateur avec les autres réseaux, de gestion et de compatibilité entre les différents protocoles d'échanges (TCP/IP, modes synchrones et asynchrones, SONET (synchronous optical network), SDH (synchronous digital hierarchy) …) . Les nœuds de ces réseaux comportent un OADM.

Le souci dans tout réseau est le risque de panne : pour éviter de bloquer toute communication, on associe souvent deux fibres, ainsi, si l'une se rompt, l'autre peut prendre le relais. Mais ceci nécessite une intervention rapide : on implémente donc dans le système un protocole de contrôle actif qui peut répondre instantanément en cas de disfonctionnement en redirigeant le trafic vers la seconde fibre, mais ceci augmente le coût global du réseau.

Pour établir un réseau de coût minimal avec un fonctionnement assuré en toutes circonstances, il existe des algorithmes informatiques qui permettent de construire des réseaux autorisant toutes les communications.

6.9.5.3.3.3. Le codage du signal

L'information transportée est codée en binaire (succession de 0 et de 1).

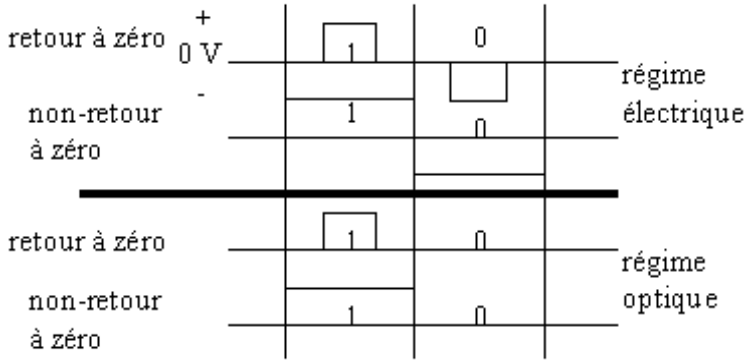


Figure : Le binaire en électrique et en optique

Les différents moyens de modulation que l'on connaît s'appliquent aussi en optique (modulation d'amplitude, modulation de fréquence et modulation de phase) :

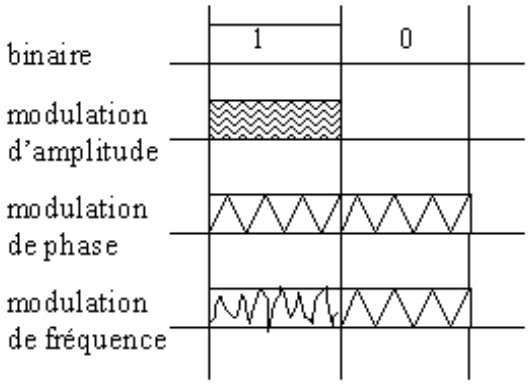


Figure : Le codage de l'information optique

Lors de la transmission cependant, un bit (0 ou 1) peut se transformer, ce qui peut créer une erreur. On pourrait alors pour éviter cela envoyer plusieurs fois le même signal (2, 3 ou plus) , mais cela consomme beaucoup de bande passante pour une efficacité limitée . On peut adopter une solution qui s'appelle le code de Hamming : à l'aide d'une matrice de codage précise, on transmet un signal, qui , à sa réception , est décodé par une matrice de décodage associée à celle de codage et assure de retrouver le signal d'origine même si une erreur a surgi . La transmission codée demande plus de bande passante que le signal simple, mais est très efficace : on minimise le taux d'erreur en n'augmentant que légèrement la quantité d'informations à transmettre.

6.9.5.3.3.4. LE MULTIPLEXAGE : Une solution d'avenir.

Le multiplexage a dépassé le stade de la recherche et est maintenant l'objet d'une attention grandissante.
Il présente notamment deux avantages principaux :
-une économie sur le coût des fibres optiques et de leur installation.
-une flexibilité dans l'élaboration du système.

6.9.5.3.3.5. Principe :

Le multiplexage de longueur d'onde : Il s'agit de superposer sur la même fibre, des signaux optiques à différentes longueurs d'onde et ainsi augmenter la capacité de transmission à un meilleur coût.
A une extrémité du réseau, se trouve le multiplexeur, le composant d'entrée. Il doit introduire dans la fibre, avec le minimum de pertes possibles, les signaux issus de différentes sources.
A l'autre extrémité de la fibre, les signaux de différentes longueurs d'ondes seront séparées spatialement par des détecteurs uniques ou différents : Le démultiplexeur.

6.9.5.3.3.5.1. Multiplexeur Démultiplexeur :

A l'heure actuelle, il existe une large gamme de multiplexeur. Chacun basé sur des conditions d'émission et de réception particulières, cependant toujours tourné vers la rapidité et le bon acheminement du message transmis.

6.9.5.3.3.5.2. Filtres multi diélectriques utilisés en multiplexage.

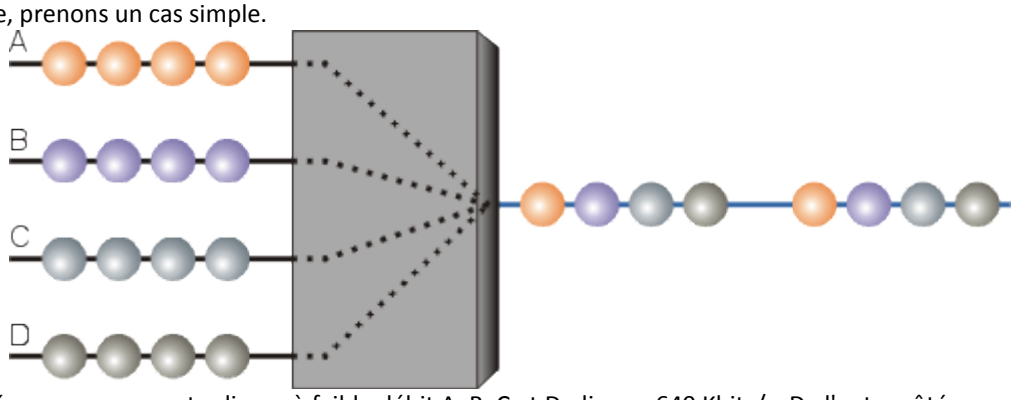
Les filtres diélectriques permettent la séparation angulaire en réfléchissant une certaine gamme de longueurs d'onde et en transmettant les autres. Les deux domaines spectraux peuvent être larges (c'est-à-dire une grande amplitude), notamment pour les filtres passe-haut et passe-bas, les plus couramment utilisées. Ces filtres sont réalisés par empilement de couches alternativement de haut (H) et de bas (L).La difficulté réside dans la nécessité de réaliser des filtres à haut pouvoir réflecteur dans un domaine de longueur d'onde donné mais possédant aussi une très bonne transmission dans le domaine de longueurs d'ondes complémentaire.

6.9.5.3.3.5.3. Réseaux de diffraction utilisés en multiplexage :

Les multiplexeurs à filtres ne peuvent pas être utilisés quand les canaux sont nombreux ou proches en longueur d'onde. Le réseau à l'avantage de traiter en même temps un grand nombre de voies avec des composants très simples dans la plupart des cas.
Un réseau se compose avant tout d'une surface optique qui transmet ou réfléchit la lumière et sur laquelle un grand nombre de traits sont gravés. Le réseau à la propriété de renvoyer, séparées angulairement, les différentes longueurs d'onde contenues dans un faisceau incident. En vertu du principe du retour inverse de la lumière, le réseau peut recombiner dans une même direction, des faisceaux incidents séparés angulairement et de longueurs adéquates. L'angle de diffraction est fonction de l'espacement des traits et de l'angle d'incidence.
Il existe bien évidemment à l'heure actuelle divers autres procédés pour le multiplexage, par exemple basés sur l'électronique moléculaire. Mais en général, les procédés les plus utilisés sont ceux décris précédemment. On peut aussi trouver des systèmes hybrides alliant à la fois les filtres et les réseaux. De même, il existe un grand nombre d'appareillage en ce qui concerne le domaine de la fibre optique, chacun présentant un procédé plus ou moins intéressant en fonction de l'utilisation voulue. Sans compter que les découvertes se multiplient, le monde de la fibre optique étant dans une phase de forte expansion au niveau de la recherche.

- Multiplexage temporel

Là encore, prenons un cas simple.

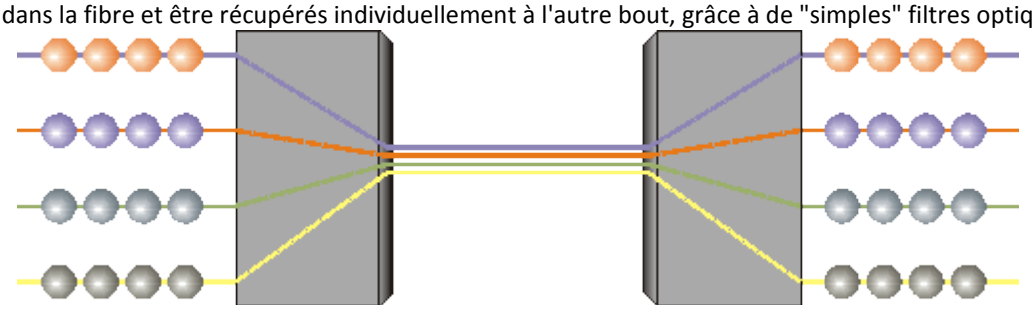


D'un côté, nous avons quatre lignes à faible débit A, B, C et D, disons, 640 Kbits/s. De l'autre côté, nous avons une fibre optique qui pourrait passer facilement 100 fois plus... Autrement dit, alors que la ligne A par exemple, va mettre une seconde à déverser 640 Kbits, la fibre optique va faire passer ces 640 Kbits en 1/100 de seconde, et va attendre 99/100 de seconde le paquet suivant en provenance de la ligne A.
Ici l'on va tout simplement utiliser un multiplexeur temporel, qui va accumuler des paquets de données provenant des lignes A, B, C et D et les passer séquentiellement sur la fibre optique.
Dit autrement, vous avez quatre petites routes, où les voitures roulent pare-chocs contre pare-chocs. Ces quatre routes débouchent sur une autoroute à 10 voies. Les routes sont saturées, mais l'autoroute peut encore accepter beaucoup d'autres voitures.
Ce type de multiplexage s'appelle TDM (Time Division Multiplexing).

Dans cette approche, nous utilisons une fibre optique avec une seule source lumineuse. C'est peut-être dommage, parce que cette fibre, à l'image d'un câble de cuivre, peut faire passer plusieurs fréquences (longueurs d'ondes), donc plusieurs couleurs.

- Multiplexage spatial

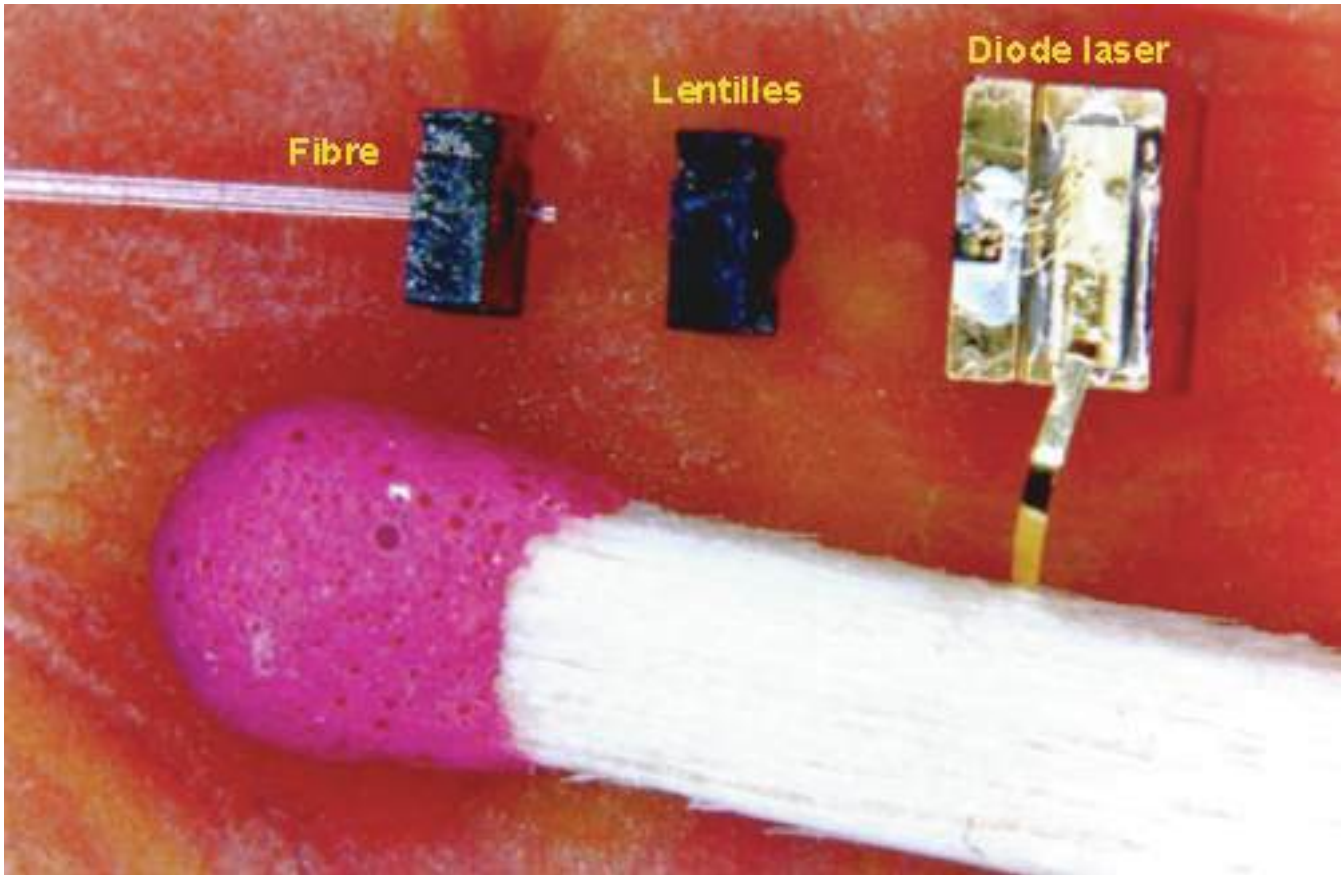
Sitôt dit, sitôt fait. Nous allons utiliser plusieurs lasers de couleurs différentes. Ces faisceaux lasers pourront voyager dans la fibre et être récupérés individuellement à l'autre bout, grâce à de "simples" filtres optiques.



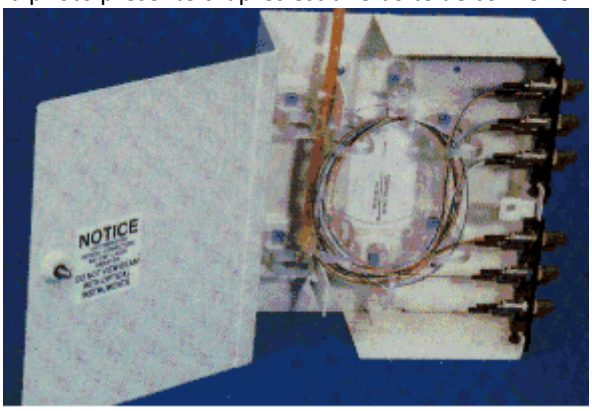
Une fibre optique peut facilement transporter des longueurs d'ondes comprises entre 1 530 nm et 1 565 nm, nous sommes dans l'infrarouge (l'illustration fait apparaître des couleurs pour la compréhension) et sur de la fibre mono mode. 35 nm d'écart, ça ne parait pas beaucoup. Oui, mais comme on sait séparer deux ondes lumineuses si la différence de longueur d'onde est de 0,8 nm et même 0,4 nm, alors, on peut passer dans la même fibre de 43 à 87 "lumières" différentes. Cette méthode s'appelle: DWDM (Dense Wavelength Division Multiplexing). Si l'on considère que l'on peut passer sans problèmes 2,5 Gbist/s sur chaque canal...
Avec cette méthode, il est même possible d'utiliser certains canaux dans un sens et d'autres canaux dans l'autre, ce qui permet de faire du "full duplex" avec une seule fibre.
Encore plus fort :
Paris, le 21 mars 2001 - Alcatel, (Paris: CGEP.PA, NYSE: ALA), leader mondial des réseaux optiques intelligents, a établi deux nouveaux records du monde pour des transmissions DWDM multi-Térabits. Le Groupe a d'une part franchi la barre mythique des 10 Tbit/s (10 000 Gbit/s), établissant le record mondial absolu de capacité de transmission sur une fibre optique. Alcatel a d'autre part réalisé une transmission record de 3 Tbit/s (3 000 Gbit/s) sur une distance transocéanique de 7 300 kilomètres. (Source Alcatel)
Mais...
Cette technique emploie:
De la fibre mono mode
Une (des) source(s) lumineuse(s) laser, ce qui est obligatoire avec ce type de fibre.
La fibre mono mode a un diamètre de l'ordre de 10 µm (1/100 de millimètre). Ce n'est pas bien gros et on devine que les technologies nécessaires pour "enfiler" un rayon laser dans cette fibre ne sont pas simples. A fortiori s'il faut en faire passer plusieurs. Et il faut aussi récupérer les signaux à l'autre bout.
En d'autres termes, les performances de cette technologie n'ont d'égal que son prix. Tout le problème consiste donc à choisir la technologie la mieux appropriée à ses besoins présents et futurs, pour ne pas se retrouver avec un réseau
Ruineux parce que la technologie utilisée, trop chère, ne peut être rentabilisée.
Ruineux parce que la technologie utilisée, trop peu performante pour une raison de prix, ne pourra pas assurer l'inévitable croissance ultérieure, autrement qu'en multipliant les équipements de bout en bout du réseau.
Les sources lumineuses

Le plus souvent, ce sont des diodes électroluminescentes. Il en existe de toutes sortes. Il en existe même qui sont capables d'émettre un faisceau laser.

Ces dispositifs ne sont pas énormes, témoin l'illustration ci dessous. L'allumette donne l'échelle.



La photo presenté ci aprés est une boite de connexion murale pour les connecteur ST



Voici les différents types de Câblage de la Fibre Optique

Prix et offres

Les coûts pour une installation

Le coût pour du câblage pour la fibre optique est très élevé. Pour un mètre de ce câblage, il faut débourser entre 50 et 100 Euros. Le coût du génie civil, c'est à dire le coût d'installations pour les câblages, serveurs et autres..., est environ entre 60 et 700 Euros par mètre de fibre optique. Pour brancher un abonné à une connexion de fibre optique, il faut en moyenne entre 10.000 et 12.000 Euros par abonnée. En comparaison, l'ADSL coûte à l'opérateur entre 200 et 1.000 Euros par abonné. Tous ces chiffres montrent le coût extrêmement élevé de la Fibre Optique.

7. Techniques de codage sur fibre optique ou paire torsadée

7.1. Introduction

On peut considérer que les techniques de codage utilisées sur les lignes de transmission constituent l'interface entre le support physique et son utilisation. Les techniques mises en œuvre participent pour beaucoup dans la performance de la transmission et dans sa capacité à utiliser le potentiel du média.

Dans une première partie, nous allons parcourir les différentes techniques de base traditionnellement utilisées et régulièrement améliorées. Elles concernent essentiellement les codages en bande de base et les différents types de modulation simples.

Puis nous décrirons ensuite les modulations et multiplexages plus sophistiqués qui ont vu le jour ces dernières années pour face aux besoins toujours croissants en débits sur les grandes artères de communication et dans la desserte locale de l'usager.

Enfin dans une troisième partie, nous étudierons les ressemblances entre les techniques utilisées sur fibre optique et sur paire torsadée. Les concepteurs de ces techniques sont parfois partis de constatations communes pour arriver à des solutions ayant des ressemblances bien que les problèmes de base et les contextes soient différents.

7.2. Les techniques de base

7.2.1. Notions de base et rappels

Transmission numérique et transmission analogique

Il convient de bien différencier l'information de la transmission.

L'information est représentative de faits, de données. Ces données peuvent être d'origine analogique ou numérique, c'est à dire représentées par une suite binaire.

Une information analogique peut être numérisée, par exemple la vidéo. Inversement, des données numériques peuvent être transformées en signaux analogiques.

Un signal est dit numérique lorsque son amplitude ne prend que des valeurs discrètes par intervalle. Il est dit analogique lorsque son amplitude varie de manière continue dans le temps.

Les codages en bande de base

Le signal binaire n'est généralement pas transmis directement sur la ligne et différents codages numériques sont utilisés pour différentes raisons :

La récupération de l'horloge nécessaire en transmission synchrone est facilitée par des séquences qui présentent des changements d'états fréquents et évitent ainsi les longues suites de 1 ou de 0. Le spectre d'un signal binaire est concentré sur les fréquences basses qui sont les plus affaiblies sur la ligne. Les perturbations subies par un signal sont proportionnelles à la largeur de sa bande de fréquence. La transmission est dite en bande de base si elle ne subit aucune transposition de fréquence par modulation. Les fréquences initiales du signal émis sont donc préservées. La transmission en bande de base ne peut donc par essence être utilisée que

sur support cuivre. Les signaux bande de base sont sujets à une atténuation dont l'importance dépend du support employé et doivent donc être régénérés périodiquement sur une longue distance.

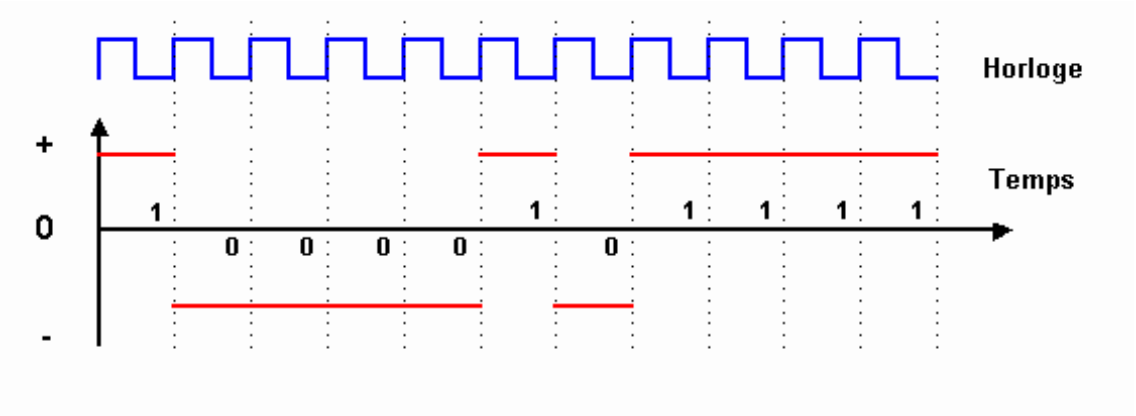
La modulation numérique
Différentes raisons rendent impossibles la transmission en bande de base à des vitesses élevées et sur de grandes distances : Pas de propagation pour les fréquences en dehors de la bande passante du support ; Pertes et affaiblissements du fait de la ligne ;
Impossibilités de différencier plusieurs communications sur un même support ; Bruit, diaphonie
Ces raisons imposent la transformation des données numériques en un signal analogique adapté au support de transmission. Trois principaux types de modulations sont utilisés en transmission.

7.2.2. Les codages

Pour l'ensemble des différents codes décrits, nous prendrons la même suite binaire afin de permettre la comparaison : 1 0 0 0 0 1 0 1 1 1 1

7.2.2.1. Codage NRZ (Non Return to Zero)

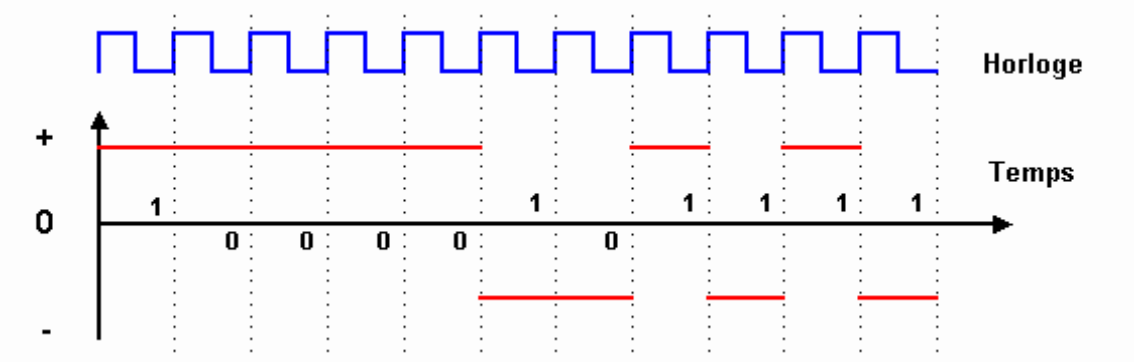
Principe : très proche du codage binaire de base, il code un 1 par +V, un 0 par -V



Le codage NRZ améliore légèrement le codage binaire de base en augmentant la différence d'amplitude du signal entre les 0 et les 1. Toutefois les longues séries de bits identiques (0 ou 1) provoquent un signal sans transition pendant une longue période de temps, ce qui peut engendrer une perte de synchronisation.
Le débit maximum théorique est le double de la fréquence utilisée pour le signal : on transmet deux bits pour un hertz.

7.2.2.2. Codage NRZI (Non Return to Zero Inverted)

Utilisation : Fast Ethernet (100BaseFX), FDDI
Principe : on produit une transition du signal pour chaque 1, pas de transition pour les 0.

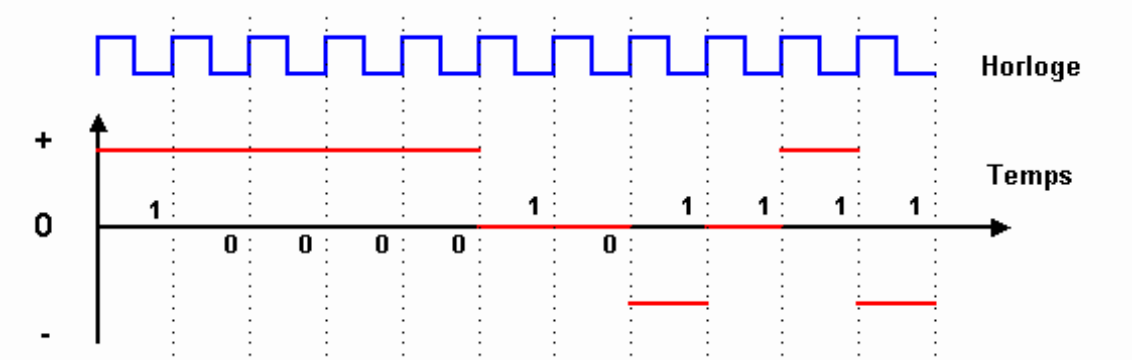


Avec le codage NRZI, on voit que la transmission de longues séries de 0 provoque un signal sans transition sur une longue période. Le débit binaire est le double de la fréquence maximale du signal : on transmet deux bits pour un hertz.

7.2.2.3. Codage MLT3

Utilisation : Fast Ethernet (100BaseTX, 100BaseT4), ATM,

Principe : Dans ce codage, seuls les 1 font changer le signal d'état. Les 0 sont codés en conservant la valeur précédemment transmise. Les 1 sont codés successivement sur trois états : +V, 0 et –V.



Le principal avantage du codage MLT3 est de diminuer fortement la fréquence nécessaire pour un débit donné grâce à l'utilisation de 3 états. Pour 100Mbps de débit, une fréquence maximale du signal de 25Mhz seulement est atteinte.

Les longues séquences de 0 peuvent entraîner une perte ou un déphasage de l'horloge du récepteur.

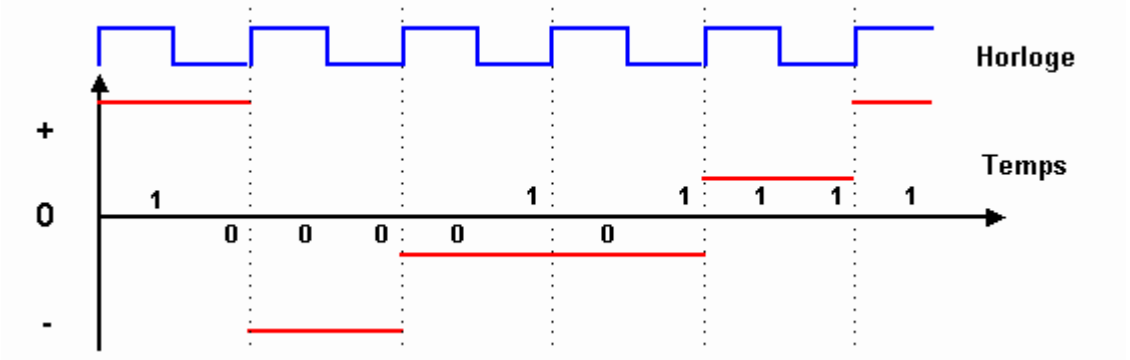
7.2.2.4. Codage 2B1Q

Utilisation : RNIS/ISDN, HDSL

Principe : Le code 2B1Q fait correspondre à un groupe de deux éléments un créneau de tension dit symbole quaternaire pouvant endosser quatre valeurs différentes suivant la table ci-dessous :

Groupe de 2 bits	Tension
00	-3
01	-1
11	+1
10	+3

Table de codage2B1Q

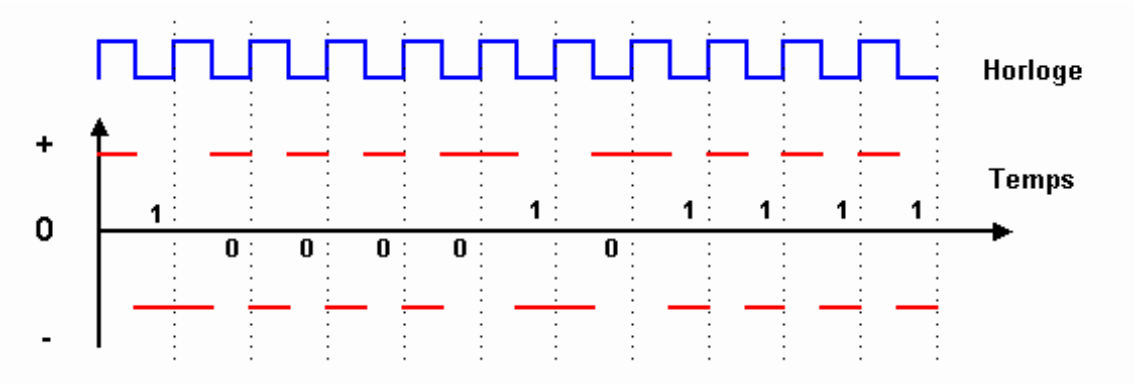


Les données sont donc transmises à deux fois la fréquence du signal.

7.2.2.5. Codage Manchester

Utilisation : Ethernet 10Base5, 10Base2, 10BaseT, 10BaseFL

Principe : dans le codage Manchester, l'idée de base est de provoquer une transition du signal pour chaque bit transmis. Un 1 est représenté par le passage de +V à –V, un 0 est représenté par le passage de -V à +V.



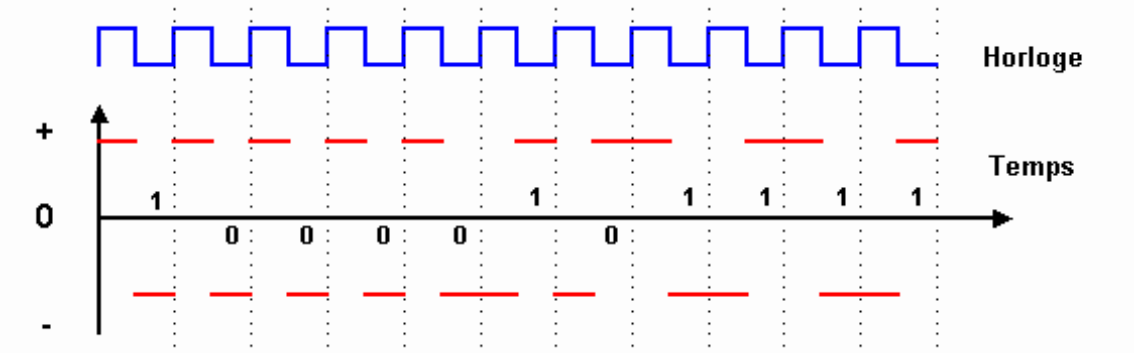
La synchronisation des échanges entre émetteur et récepteur est toujours assurée, même lors de l'envoi de longues séries de 0 ou de 1. Par ailleurs, un bit 0 ou 1 étant caractérisé par une transition du signal et non par un état comme dans les autres codages, il est très peu sensible aux erreurs de transmission. La présence de parasites peut endommager le signal et le rendre incompréhensible par le récepteur, mais ne peut pas transformer accidentellement un 0 en 1 ou inversement.

Toutefois, le codage Manchester présente un inconvénient : il nécessite un débit sur le canal de transmission deux fois plus élevé que le codage binaire. Pour 10 Mbit/s transmis, on a besoin d'une fréquence à 10 Mhz. Ceci le rend difficilement utilisable pour des débits plus élevés. L'utilisation de ce codage pour une transmission à 1 Gbit/s nécessiterait une fréquence maximale du signal de 1 Ghz, ce qui est incompatible avec les possibilités des câblages actuels ainsi qu'avec les normes sur les compatibilités électromagnétiques. Plus la fréquence du signal est élevée, plus les phénomènes de paradiaphonie pouvant perturber les installations avoisinantes du câble sont sensibles. Les normes ISO 11801 et EN 50173 fixent entre autres les règles de compatibilité électromagnétiques (EMC : Electro Magnetic Compatibility).

7.2.2.6. Codage Manchester différentiel

Utilisation : Token Ring

Principe : c'est la présence ou l'absence de transition au début de l'intervalle du signal d'horloge qui réalise le codage. Un 1 est codé par l'absence de transition, un 0 est codé par une transition au début du cycle d'horloge.



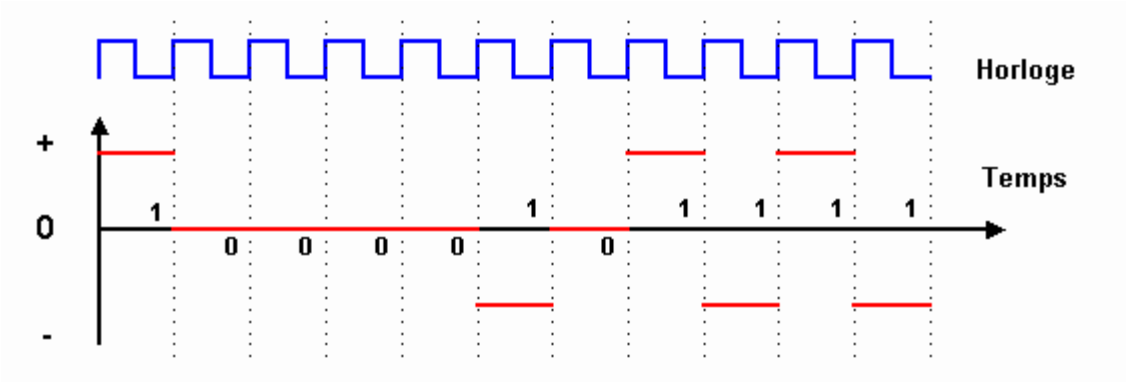
A noter la présence de deux symboles particuliers : J et K. Ils sont codés par +V et –V sur toute la durée d'un cycle d'horloge. Ils ont pour but de marquer le début et la fin d'une trame

Le codage présente le même inconvénient que le codage Manchester : nécessite une fréquence égale à celle du débit utile. Il présente par contre un avantage : ce sont les transitions du signal et non pas ses états qui représentent les bits transmis, il est donc insensible aux inversions de fils dans le câblage.

7.2.2.7. Codage bipolaire ou AMI (Alternate Mark Inversion)

Utilisation : Lignes DS1/T1

Principe : Les 0 sont représentés par des potentiels nuls, les 1 par +V et –V en alternance.

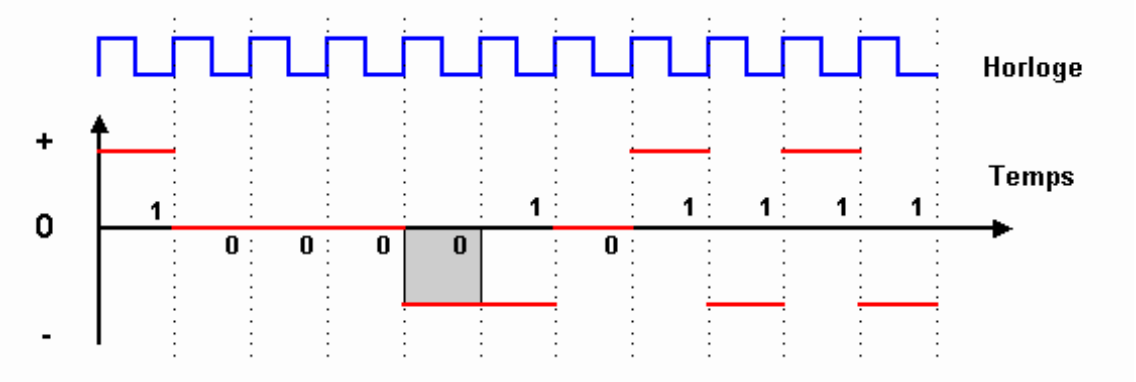


Ici encore, il peut y avoir de longues séquences sans potentiel et donc perte de synchronisation.

7.2.2.8. Codage HDBn (Haute Densité Binaire d'ordre n) ou BnZs (Bipolar with n Zero Substitution)

Utilisation : HDB3 : E1, E3 ; B8ZS : T1 ; B3ZS : T3

Principe : le principe de base est le même que pour le codage bipolaire, mais pour éviter une trop longue série de 0, on introduit un bit supplémentaire au signal pour terminer une série de n 0 consécutifs. Ce bit supplémentaire est de même phase que le dernier 1 transmis pour pouvoir l'identifier, afin qu'il ne soit pas pris en compte dans l'information transmise.

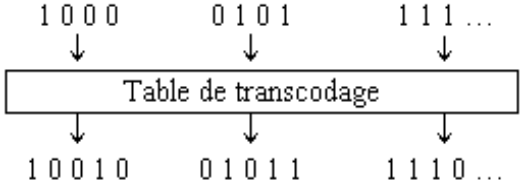


7.2.2.9. Codage nB/mB

Utilisation : 4B/5B : Fast Ethernet ; 8B/10B : Gigabit Ethernet

Principe : Il s'agit d'un codage par bloc. On utilise une table de transcodage pour coder un groupe de n bits en m bits, avec m < n. Ce codage ne définit pas la mise en ligne des bits. On utilise généralement pour cela un codage de type NRZI ou MLT3.

La suite binaire 1 0 0 0 0 1 0 1 1 1 1 précédemment utilisée va être découpée en groupes de 4 bits. La table de transcodage ci-dessous permet de transformer chaque groupe de 4 bits en groupe de 5 bits.



La suite à transmettre ne comporte pas plus de deux 0 consécutifs, ce qui la rend plus facile à transmettre un fois codée en NRZI ou MLT3.

Groupe de 4 bits	Symbole 4B5B
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

Table de transcodage 4B5B

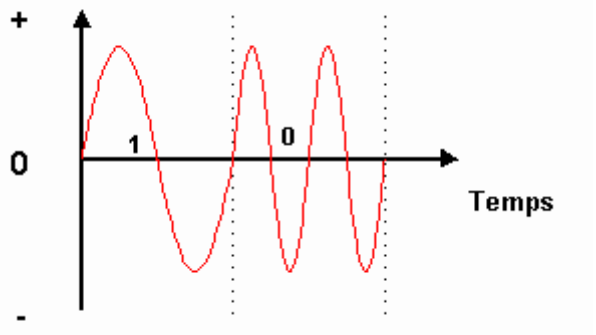
Ce type de codage apporte la garantie de ne pas avoir à transmettre plus de deux 0 successifs. Les caractères spéciaux, hors données utiles, peuvent trouver leur place dans la table de transcodage sans nécessiter un état spécial du signal comme dans les codages Manchester.

Le codage 4B5B augmente la fréquence du signal. Par exemple 125Mhz pour 100Mbps. Associé à un codage de type NRZI, on obtient dans le cas du Fast Ethernet (100BaseFX) une fréquence de 62.5Mhz. Avec un codage MLT3, la fréquence du signal tombe à 31.25Mhz pour le Fast Ethernet 100BaseTX.

Par ailleurs ce type de codage laisse un nombre important de mots de 5 bits inutilisés. Même en éliminant les groupes pouvant poser des problèmes de transmission comme 00000 par exemple, il reste des mots pouvant être utilisés pour le contrôle de la transmission ou d'autres fonctions comme début ou fin de paquet par exemple.

7.2.3. Les modulations de base

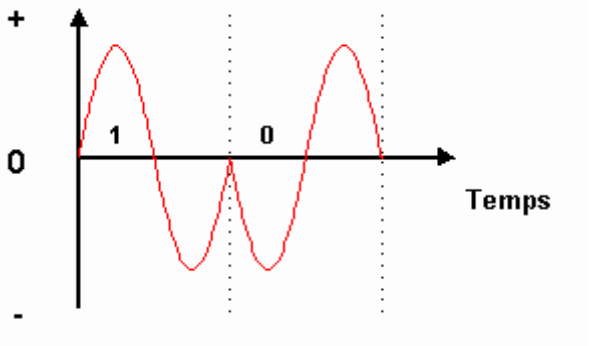
7.2.3.1. Modulation de fréquence ou FSK (Frequency Shift Keying)



En modulation de fréquence, les niveaux logiques sont représentés par la variation de la fréquence de la porteuse. Par exemple :

La modulation FSK est utilisée pour des transmissions à faible débit sur le réseau téléphonique commuté.

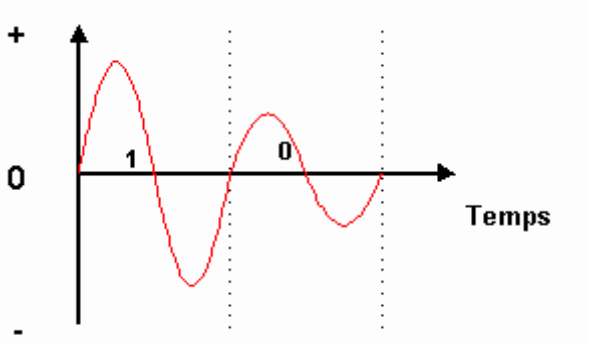
7.2.3.2. Modulation de phase ou PSK (Phase Shift Keying)



La modulation de phase associe à un code binaire une valeur de la phase de la porteuse. La vitesse peut être facilement augmentée en utilisant un code binaire sur 2, 3 bits ou plus sans augmentation de la fréquence de la porteuse.

7.2.3.3. Modulation d'amplitude ou ASK (Amplitude Shift Keying)

La modulation d'amplitude s'applique en faisant varier l'amplitude du signal en fonction des bits à coder. Par exemple :



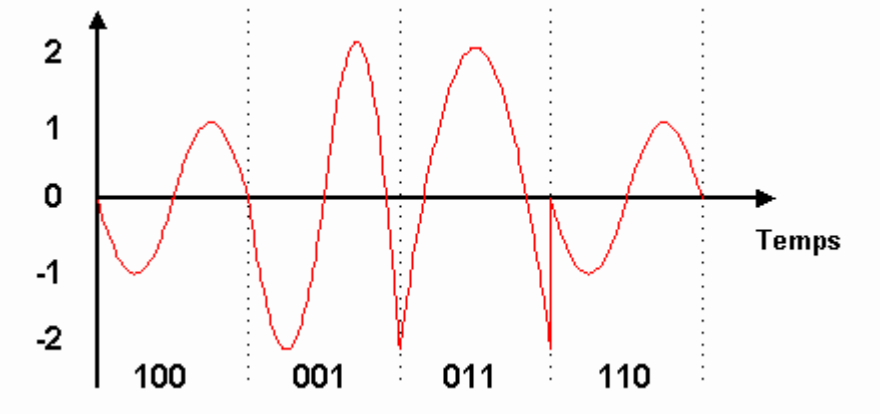
A noter que la modulation d'amplitude est la seule utilisable sur fibre optique, car les équipements utilisés actuellement ne sont pas en mesure d'appliquer une autre modulation sur les ondes lumineuses. Dans ce cas, la modulation s'effectue par tout ou rien.
Par contre, elle est peu employée sur d'autres supports, car elle provoque une détérioration du rapport signal sur bruit.

7.2.3.4. Modulation QAM

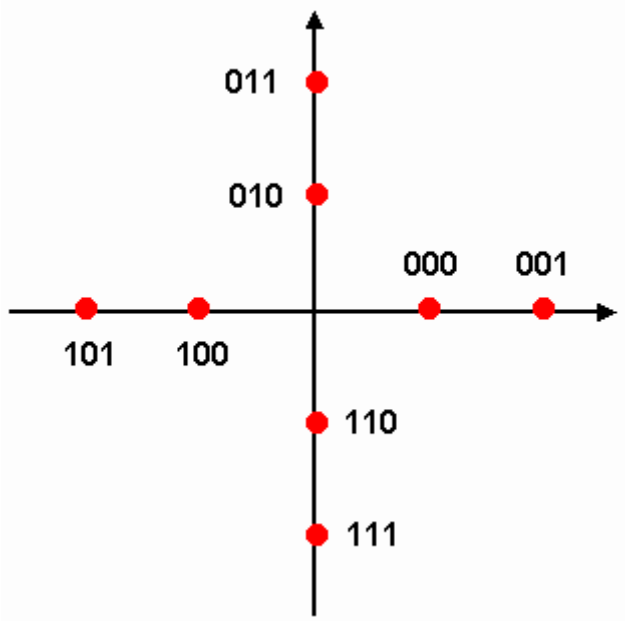
La modulation QAM (Quadrature Amplitude Modulation) ou modulation d'amplitude en quadrature de phase est une technique qui emploie une combinaison de modulation de phase et d'amplitude. Elle est largement employée par les modems pour leur permettre d'offrir des débits binaires élevés.
Prenons par exemple un signal modulé QAM avec 3 bits transmis par baud. Une telle modulation requiert donc 2^3 soit 8 combinaisons binaires différentes. Dans notre exemple, nous prendrons 2 amplitudes combinées avec 4 décalages de phase différents. La table de correspondance pourra être du type :

Groupe de bit	Amplitude	Décalage de phase
000	1	0
001	2	0
010	1	¼
011	2	¼
100	1	½
101	2	½
110	1	¾
111	2	¾

Exemple de codage de la suite binaire 1 0 0 0 0 1 0 1 1 1 1 0 à partir de la table ci-dessus :



Les combinaisons possibles en modulations QAM sont souvent représentées par une constellation de points représentant chacun un groupe de bits.



Exemple de constellation QAM8 (3 bits par baud)

Dans une constellation QAM, l'éloignement du point par rapport à l'origine indique l'amplitude, son angle indique le décalage de phase. Chacun des canaux définis par le multiplexage DMT en ADSL est modulé en QAM sur 15 bits au maximum. 32768 combinaisons d'amplitudes et de décalages de phase sont donc nécessaires.
Il existe également une variante de la modulation QAM, la modulation codée en treillis TCM (Trellis Coded Modulation). Ce type de modulation est utilisé pour les modems rapides (V32, V34, V90).

8. Le protocole IP

Le Protocole Internet ou IP (Internet Protocol) est la partie la plus fondamentale d'Internet. Si vous voulez envoyer des données sur Internet, vous devez les "emballer" dans un *paquet IP*. Je parlerai plus loin de ces paquets IP. Il faut savoir pour l'instant que ces derniers ne doivent pas être trop gros; la plupart du temps, ils ne peuvent pas contenir toute l'information qu'on voudrait envoyer sur Internet, et cette dernière doit par conséquent être fractionnée en de nombreux paquets IP.
Les paquets IP, outre l'information, sont constitués d'un en-tête contenant l'adresse IP de l'expéditeur (votre ordinateur) et celle du destinataire (l'ordinateur que vous voulez atteindre), ainsi qu'un nombre de contrôle déterminé par l'information emballée dans le paquet : ce nombre de contrôle, communément appelé *en-tête de total de contrôle*, permet au destinataire de savoir si le paquet IP a été "abîmé" pendant son transport.

8.1. L'adresse IP

Une des choses les plus intéressantes du protocole TCP/IP est d'avoir attribué un numéro fixe, comme un numéro de téléphone, à chaque ordinateur connecté sur Internet; ce numéro est appelé l'*adresse IP*. Dans le cadre du standard actuel - IPV4 -, les adresses sont codées sur 32 bits. Ainsi, tout ordinateur sur Internet, par exemple le vôtre lorsque vous vous connectez par l'entremise de votre provider, se voit attribuer une adresse de type a.b.c.d (où a,b,c,d sont des nombres compris entre 0 et 255), par exemple 202.15.170.1. Dès ce moment, vous êtes le seul au monde à posséder ce numéro, et vous y êtes en principe directement atteignable.

Un rapide calcul vous montre qu'il y a, en théorie, un maximum de 256^4 = 4'294'967'296 adresses possibles, ou, en d'autres termes, d'ordinateurs directement connectables, ce qui est plus que suffisant même à l'échelle mondiale (du moins à l'heure actuelle !). En fait, il y a *beaucoup* moins d'adresses que ce nombre impressionnant, car de nombreux numéros IP ne sont pas autorisés ou sont utilisés à des fins "techniques".
Pour l'ordinateur, cette adresse IP est codée en binaire (4 x 8 bits = 32 bits). Par exemple,

202	15	170	1
11001010	00001111	10101010	00000001

Il est clair que pour nous les humains, il est plus facile de retenir 202.15.170.1 que 11001010000011111010101000000001 !

8.2. Les différents types de réseaux

L'adressage a été structuré logiquement dans une architecture de réseaux et de sous-réseaux. N'importe qui ne peut s'approprier librement une adresse IP : ces dernières sont régies par un organisme international, l'Internic, qui délivre les différentes adresses ou plutôt les classes de réseaux.
Dans un réseau de classe A, l'Internic fixe les 8 premiers bits (dits bits de poids fort) sous la forme 0xxxxxxx; les 24 autres bits sont laissés à l'administration de l'acquéreur du réseau de classe A. Dans un tel réseau, les adresses IP sont donc de type F.b.c.d où F (fixé par L'Internic) va de 0 à 126, les valeurs b, c et d étant laissées librement administrables par l'acquéreur. De grandes sociétés ont ce type de réseau; par exemple, Hewlett-Packard possède le réseau 16.b.c.d (qu'on note aussi 16.0.0.0). Vous noterez que seuls 127 réseaux de ce type sont disponibles.
Dans un réseau de classe B, l'Internic fixe les 16 premiers bits sous la forme 10xxxxxx yyyyyyyy, ce qui donne des réseaux de type F.G.0.0 où F (128-191) et G (0 à 255) sont fixés par le NIC.
Dans un réseau de classe C, l'Internic fixe les 24 premiers bits sous la forme 110xxxxx yyyyyyyy zzzzzzzz, ce qui donne des réseaux de type F.G.H.0 où F (192-223), G et H (0-255) sont fixés par le NIC.
Tout le réseau 127.0.0.0 (qu'on peut voir comme un réseau de classe A) n'est pas attribué par l'Internic, car l'adresse 127.0.0.1, dite *adresse de boucle*, est réservée à des fins techniques. Dommage, car 24 millions d'adresses sont ainsi perdues !
De plus, l'Internic n'attribue pas non plus certains réseaux qui sont laissés à des fins privées. Ces plages d'adresses généralement non routées par les fournisseurs d'accès, en d'autres termes des plages attribuables tout à fait légalement pour des réseaux internes, vont
de 10.0.0.0 à 10.255.255.255
de 172.16.0.0 à 172.31.255.255
de 192.168.0.0 à 192.168.255.255
Typiquement, si vous créez votre propre réseau local en TCP/IP, vous utiliserez pour vos ordinateurs ce type d'adresses. Je reparle de ce cas dans la partie sur la façon de configurer un réseau local et le connecter à Internet.

Il me faut encore rajouter que certaines adresses d'un réseau quelconque ne sont pas attribuables à un ordinateur précis, mais joue un rôle "technique" dans TCP/IP.
Prenons l'exemple d'un réseau de classe C comme 192.168.0.x, x pouvant varier entre 0 et 255.
Cette plage d'adresses doit être indiquée de manière officielle, et on utilise pour cela l'adresse générale 192.168.0.0, ce qui veut dire "toutes les adresses comprises entre 192.168.0.0 et 192.168.0.255". Remarquez que cela signifie que vous ne pourrez jamais attribuer l'adresse 192.168.0.0 à un ordinateur précis, puisque ce dernier fait référence à tout le réseau.
Il existe une autre adresse IP réservée : *l'adresse de diffusion (broadcast).* C'est la dernière adresse du sous réseau, dans notre cas 192.168.0.255. Il s'agit de l'adresse que vous utilisez pour diffuser un message vers chaque ordinateur du sous réseau concerné.
Finalement, ce qui sera l'objet du paragraphe 6, vous devez réserver une *adresse IP du routeur par défaut (gateway)* : c'est l'adresse "passerelle" qui permettra à des paquets IP de "quitter" votre sous réseau.

8.3. La subdivision en sous réseaux

Comment un ordinateur transmet-il l'information (les paquets IP) à son destinataire ? Une partie de la réponse se trouve dans le fonctionnement du protocole IP.
Généralement, un ordinateur ne peut transmettre directement un paquet IP qu'à un ordinateur situé sur le même sous réseau. Par exemple, un ordinateur possédant l'adresse IP 192.168.0.2 pourra directement envoyer de l'information à un ordinateur "voisin" d'adresse 192.168.0.20, mais il ne pourra pas le faire avec un ordinateur d'adresse 194.38.175.55. Pour simplifier, on dira en première approche qu'un ordinateur ne peut communiquer directement qu'avec un ordinateur possédant les trois premiers nombres de l'adresse IP identiques. Cette remarque n'est malheureusement pas théoriquement juste (même si en pratique, c'est assez souvent le cas pour des réseaux simples). En fait, c'est le concept de *masque de sous réseau* qui définit ce qu'un ordinateur peut "voir" ou ne pas voir.
Le masque de sous réseau que vous avez peut-être eu l'occasion d'utiliser, si vous utilisez TCP/IP pour un réseau local, est 255.255.255.0. Ce masque veut dire que l'ordinateur concerné peut "voir" (ou communiquer avec) tous les ordinateurs possédant les trois premiers nombres de l'adresse IP identiques, comme je l'ai indiqué à l'exemple précédent. Comment fonctionne ce système à première vue aussi compliqué ?
En fait, admettons que l'ordinateur A d'adresse IP 199.34.57.10 veuille envoyer un paquet IP à l'ordinateur B d'adresse IP 199.34.57.20. A priori, A ne sait pas s'il peut communiquer directement avec B. Pour cela, il utilise le masque de sous réseau 255.255.255.0 qu'on lui a imposé. Il "convertit" le tout en binaire, ce qui donne :

11111111	11111111	11111111	00000000	masque sous réseau
11000111	00100010	00111001	00001010	adresse de A
11000111	00100010	00111001	00010100	adresse de B

L'ordinateur A doit s'assurer que partout où le masque de sous réseau a une valeur de 1, la valeur binaire de son adresse IP corresponde à celle de B. Dans l'exemple ci-dessus, il n'est pas difficile de voir que c'est le cas; finalement, les 8 derniers bits de valeur 0 indiquent que le dernier nombre de l'adresse IP est indifférent pour A : ce dernier verra donc tous les ordinateurs d'adresse 199.34.57.x, x étant compris entre 0 et 255.
Cet exemple paraît trivial, pourtant de nombreux réseaux comportent des masques de sous réseaux moins compréhensibles (pas uniquement des 0 et des 255), comme par exemple 255.255.255.224. Si vous refaites le même raisonnement, vous verrez qu'avec un tel masque, l'ordinateur 192.168.0.2 ne peut directement communiquer avec l'ordinateur 192.168.0.100 ! En fait, les 256 adresses de ce réseau de classe C seront comme subdivisées en 8 sous réseaux de 32 ordinateurs
Ainsi, les ordinateurs 192.168.0.0 à 192.168.0.31 pourront communiquer entre eux,
de mêmes que les ordinateurs 192.168.0.32 à 192.168.0.63,
les ordinateurs 192.168.0.64 à 192.168.0.95,
les ordinateurs 192.168.0.96 à 192.168.0.127,
les ordinateurs 192.168.0.128 à 192.168.0.159,
les ordinateurs 192.168.0.160 à 192.168.0.191,
les ordinateurs 192.168.0.192 à 192.168.0.223,
et les ordinateurs 192.168.0.224 à 192.168.0.255,
mais ces sous réseaux ne pourront pas communiquer directement entre eux.
Cette subdivision d'un réseau de classe C en plusieurs sous réseaux peut être utile pour un fournisseur d'accès. Vous pouvez calculer aisément les masques de sous réseaux suivants selon le nombre de sous réseaux que vous souhaitez créer.

nombre de sous réseaux	IP par sous réseau	masque de sous réseau
1	256	255.255.255.000
2	128	255.255.255.128
4	64	255.255.255.192
8	32	255.255.255.224
16	16	255.255.255.240
32	8	255.255.255.248

En fait, nous avons vu au paragraphe précédent que pour chaque sous réseau il faut déduire trois adresses IP non attribuables à un ordinateur :
L'adresse de sous réseau (généralement le premier IP du sous réseau), par exemple a.b.c.0 pour un réseau composé d'un seul sous réseau, ou a.b.c.64 pour le troisième sous réseau d'un réseau divisé en 8 sous réseaux.
L'adresse de diffusion (généralement le dernier IP du sous réseau), par exemple, en reprenant les deux exemples précédents, a.b.c.255 ou a.b.c.95.
L'adresse du routeur par défaut dont je parle un peu plus loin, par exemple a.b.c.1 ou a.b.c.65.
Chaque sous réseau "perd" donc trois adresses IP; il s'ensuit qu'une subdivision excessive d'un réseau n'est pas avantageuse (on divise rarement au-delà de 8 sous réseaux).

8.4. Le routage des paquets IP et le protocole TCP

Revenons à notre ordinateur A d'adresse 192.168.0.2 (mettons-lui un masque de sous réseau de 255.255.255.0). Admettons qu'il veuille envoyer un paquet IP à ordinateur B d'adresse 192.170.0.4. En utilisant le masque de sous réseau, A comprend qu'il ne peut atteindre directement B. Que fait-il donc ? Il envoie sans réfléchir le paquet IP à l'adresse du routeur par défaut (disons que ce dernier a été défini comme 192.168.0.254).
Qu'est-ce que ce *routeur* ? Le routeur est une machine pouvant "jouer sur plusieurs sous réseaux" en même temps. Typiquement, si on utilise un ordinateur, ce dernier possèdera deux cartes réseaux (ou plus), l'une connectée sur l'un des sous réseaux (dans notre cas, disons qu'elle possède l'adresse 192.168.0.254), l'autre connectée sur l'autre sous réseau (disons 192.170.0.192). S'il utilise le bon logiciel, un tel ordinateur est capable de faire transiter des paquets IP du réseau 192.168.0.0 vers le réseau 192.170.0.0, et inversement bien sûr.
Deux petites remarques s'imposent. Tout d'abord, vous l'aurez compris, c'est donc grâce à des routeurs que différents sous réseaux d'un réseau de classe C peuvent communiquer entre eux, par exemple l'ordinateur 192.168.0.2 avec l'ordinateur 192.168.0.120 d'un réseau de classe C subdivisé en 8 sous réseaux (masque de sous réseau 255.255.255.224). La seconde remarque est d'ordre plus pratique : vous retiendrez que Windows 95 n'est pas capable de faire du routage, bien qu'il soit tout à fait possible d'installer deux cartes réseaux (avec des IP différents) dans un ordinateur tournant sous ce système; par contre, Windows NT 4.0, même en version Workstation, est capable d'une telle fonction.
Question pertinente : pourquoi subdiviser et ne pas faire de "méga" réseaux ?
Les deux points suivants expliquent en partie pourquoi on procède ainsi.
Limiter le trafic sur un tronçon donné. Imaginons deux réseaux locaux A et B séparés par un routeur. Lorsque des ordinateurs de A discutent avec des ordinateurs de B, le routeur a pour rôle de transmettre l'information du réseau A vers le réseau B (et inversement). Par contre, si des ordinateurs de A s'échangent entre eux des données, il n'y a pas de raison qu'ils encombrent inutilement le trafic sur le réseau B, et c'est bien pour cette raison que les réseaux A et B sont distincts.
Autre évidence : si le réseau A tombe en panne, le réseau B n'en est pas affecté. C'est d'ailleurs l'avantage principal de subdiviser : éviter qu'un ennui technique qui pourrait rester localisé ne perturbe la totalité du réseau
Autre aspect non négligeable : le *broadcast (diffusion)*. Vous ne le savez peut-être pas, mais dans votre dos, les ordinateurs sont de grands bavards : ils ne cessent de causer entre eux pour signaler leur présence ou se mettre d'accord sur les protocoles qu'ils sont capables de comprendre. Pensez un peu si Internet n'était constitué que d'un seul segment : le broadcast seul des ordinateurs utiliserait l'intégralité de la bande passante avant même qu'un seul octet de données ait pu être transmis ! Pour cette raison, le travail des routeurs est non seulement de faire transiter les paquets IP, mais aussi de filtrer le broadcast local qui n'intéresse pas la planète entière. Vous comprendrez par là que les routeurs jouent un rôle essentiel pour éviter la saturation du trafic.
Disons encore quelques mots sur l'acheminement des paquets IP. Vous comprenez maintenant que lorsqu'un ordinateur doit acheminer un paquet IP, il vérifie tout d'abord s'il peut le transmettre directement (grâce au masque de sous réseau); s'il ne peut pas, il l'envoie bêtement, sans réfléchir, au routeur par défaut. A partir de

là, les routeurs sont généralement configurés pour savoir où diriger les paquets IP qui leur sont confiés; les routeurs bavardent entre eux (à l'aide de protocoles particuliers de routage, RIP ou OSPF par exemple) pour savoir quelle est la meilleure route (la plus courte généralement) pour qu'un paquet IP atteigne sa destination. De même, si une route est soudainement interrompue, les routeurs sont capables de se reconfigurer et proposer des nouvelles routes de secours.
Or le protocole IP néglige un point crucial : il ne vérifie nullement le bon acheminement des paquets IP. En d'autres termes, l'ordinateur expéditeur, dans le protocole IP, ne fait qu'envoyer le paquet IP plus loin; il ne s'intéresse pas du tout de savoir si le paquet a bien été reçu ou s'il a été endommagé pendant le transfert ! Qui doit donc assurer l'intégrité point à point, si ce n'est IP ? La réponse : son copain, TCP.
Le protocole de contrôle de transmission ou TCP (Transmission Control Protocol) vérifie donc le bon acheminement d'un paquet IP. Cela se fait de la façon suivante. Admettons que A veuille transmettre un paquet IP à B. A envoie (un peu à l'aveugle) son paquet IP à B, un peu comme une bouteille à la mer. Tant que A ne recevra pas un accusé de réception de B lui indiquant que ce dernier a bien reçu le paquet IP dans son intégrité (grâce à l'en-tête de total de contrôle), il renverra à intervalles réguliers le même paquet IP à B. Il n'arrêtera d'envoyer ce paquet qu'à la confirmation de B. Ce dernier agira ensuite de même s'il doit transmettre le paquet plus loin. Si B constate que le paquet qu'il a reçu est abimé, il n'enverra pas de confirmation, de manière à ce que A lui renvoie un paquet "neuf".
TCP fournit d'autres services sur lequels je ne m'attarderai pas ici. On résumera rapidement les principales fonctionnalités du protocole TCP ainsi :
l'établissement d'une liaison
le séquençage des paquets
le contrôle de flux
la gestion d'erreurs
le message d'établissement d'une liaison
On entend par "contrôle de flux" la capacité de TCP, entre autres, de reconstituer l'information originale à partir de paquets IP arrivés (souvent) dans le désordre le plus absolu.
C'est aussi TCP qui gère la notion de "sockets" (ports) dont je parle dans la partie concernant la façon de configurer un réseau local et le connecter à Internet.

8.5. Le système de désignation de noms (DNS)

Pour communiquer avec un autre ordinateur, il vous faut connaître son adresse IP. Or, lorsque vous "surfez" sur le net, vous écrivez très rarement de tels numéros dans votre browser. C'est tout simplement que vous faites appel, sans le savoir, à un serveur DNS.
Un serveur DNS est simplement une machine qui associe le numéro IP à une adresse plus facilement mémorisable, bref une sorte d'annuaire téléphonique pour Internet. Ainsi, la machine qui répond lorsque vous tapez http://www.microsoft.com dans votre browser possède en fait l'adresse IP 207.68.137.65. Si vous tapiez http://207.68.137.65, vous obtiendriez exactement le même résultat. Un (ou plusieurs) serveur DNS se trouvent généralement chez votre provider; vous avez d'ailleurs sûrement reçu une feuille de configuration vous indiquant une ou deux adresses IP pour ces serveurs lors de la configuration de votre connexion à votre provider.
Une manière simple de constater l'utilité d'un serveur DNS est d'ouvrir (sous Windows 95) une fenêtre DOS, et de taper ping 'adresse de l'hôte', par exemple ping www.microsoft.com. "Ping" est une fonction très utile dans l'établissement de réseau : c'est une commande qui envoie un paquet IP tout simple à un ordinateur et lui demande simplement de répondre.
Sous Windows 95, quatre paquets IP sont envoyés, et si vous avez avez tapé 'ping www.microsoft.com' par exemple, votre ordinateur devrait ensuite vous écrire une ligne de type :
pinging www.microsoft.com [207.68.137.65] with 32 bytes of data
suivie de quatre lignes de la forme : reply from 207.68.137.65: bytes=32 time=550ms TTL=128
Ces quatre dernières lignes vous indiquent que le serveur Microsoft a répondu à vos appels et vous montrent le temps total qu'a pris la transaction pour chaque ping (par exemple 550 millisecondes). Vous noterez surtout que le serveur DNS de votre provider aura fait automatiquement la translation www.microsoft.com **<->** 207.68.137.65.
PS : J'ai parlé plus haut de l'adresse IP réservée 127.0.0.1, dite adresse de boucle; un ping sur cette adresse correspond à un ping "sur soi-même", ce qui permet de tester la bonne marche de la carte réseau.

9. Wi-Fi

9.1. TRANSMISSION RADIO

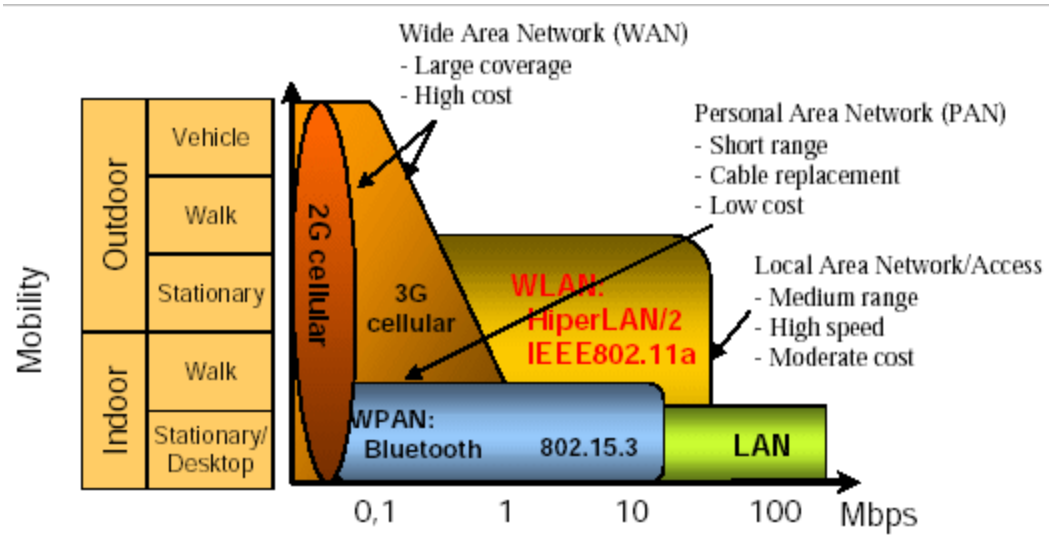
9.1.1. GENERALITES

9.1.1.1. Introduction :

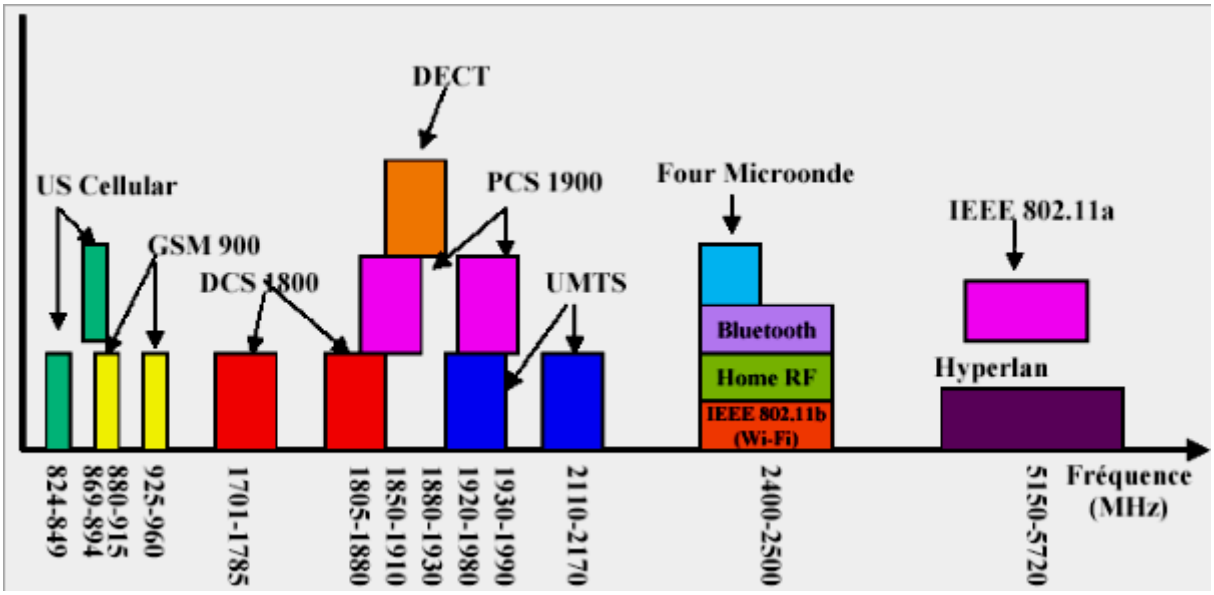
Les technologies sans fil, de même que les liaisons filaires, se regroupent en trois catégories suivant la portée de ces liaisons :

- les WWAN (Wireless Wide Area Network): GSM, GPRS, UMTS
- les WLAN (Wireless Local Area Network) RLAN (RadioLan):IEEE 802.11, Hiperlan
- les WPAN (Wireless Personal Area Network): Bluetooth, HomeRF

Le WPAN couvre quelques mètres, le WLAN se mesure en dizaines et en centaines de mètres, le WWAN en centaines et en milliers de mètres.



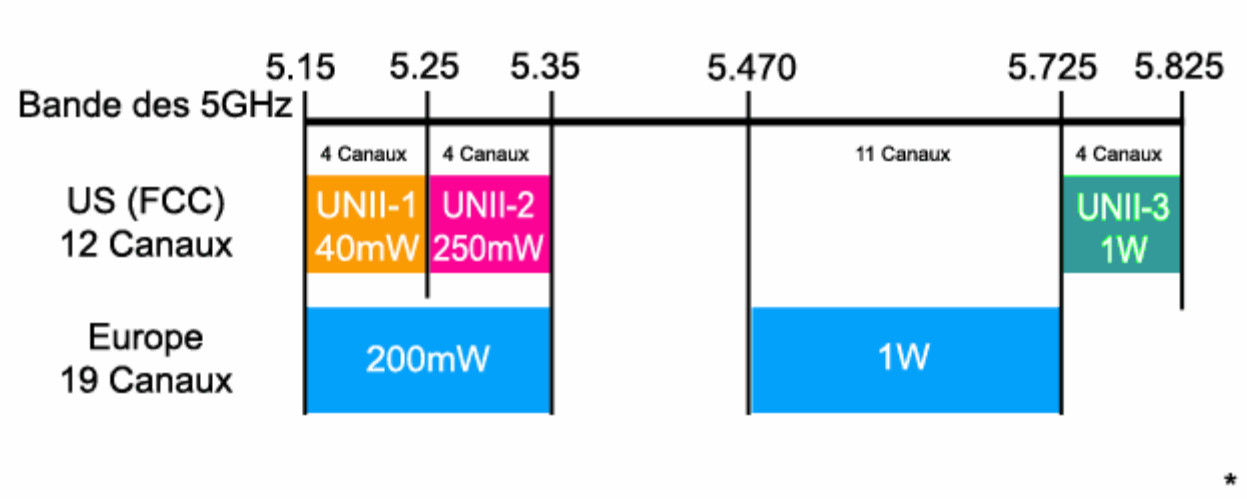
9.1.1.2. Les bandes de fréquences :



Deux groupes sont représentés :

- les technologies pour les téléphones portables (de 824 à 2170 MHz)

- les technologies utilisées pour l'informatique, pour les WPAN et les WLAN, fonctionnent sur deux bandes : la bande ISM (Industrial Scientific Medical) (de 2400 à 2500 MHz) et la bande U-NII (Unlicensed-National Information Infrastructure) (de 5150 à5720 MHz).
- Bande ISM :
  La bande ISM correspond à trois sous bandes (902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz) seule la bande de 2.400-2.4835 GHz, avec une bande passante de 83,5 MHz, est utilisée par la norme 802.11.
  La largeur de bande ISM (le maximum est de 83 .5MHz) est variable suivant les pays, de même que la puissance utilisable. Par ailleurs cette bande, plus précisément la sous-bande 2.400-2.4835 GHz, est fortement utilisée par différents standards et perturbée par des appareils (four à micro ondes, clavier et souris sans fil…) fonctionnant dans ces fréquences.
- Bande U-NII :
  La bande U-NII (5 .15-5.35 GHz, 5.725-5.825 GHz) offre une bande passante totale de 300MHz, chacune utilisant une puissance de signal différente.



*

9.1.2. Organismes

9.1.2.1. Les organismes de réglementation :

Ces bandes sont reconnues par les organismes de réglementations internationaux pour une utilisation sans licence. Ces organismes sont :
FCC : Federal Communication Commission pour les Etats-Unis, ETSI : European Telecommunications Standards Institute pour l'Europe, MKK : pour le Japon, ART : Autorité de Régulation des Télécommunications pour la France.

9.1.2.2. Réglementation française :

Depuis le 25 Juillet 2003, pour la France, l'ART a redéfinit l'utilisation des bandes ISM et U-NII, en fonction d'une part de la libération de la bande ISM et d'une partie de la bande U-NII par le ministère de la défense et d'autre part pour une mise en conformité sur les nouvelles directives européennes (dites " paquet Télécom "). Il est à noter que la bande ISM est dite libre c'est-à-dire qu'elle est exempte pour l'instant de toute taxe que ce soit pour un usage privé ou public. De plus il n'y a plus d'autorisation pour l'utilisation de la bande ISM en extérieur, seule une déclaration est à fournir pour un usage public.
Ces dispositions sont temporaires et serviront de cadre expérimental en attendant la création d'une loi.
Tableaux résumant les dispositions de l'ART :
Conditions techniques d'utilisation des fréquences : Les puissances sont exprimées en PIRE = puissance isotrope rayonnée équivalente, puissance de rayonnement moyenne du point d'émission en sortie d'antenne.

CONDITIONS TECHNIQUES D'UTILISATION DES FRÉQUENCES RLAN EN MÉTROPOLE		
Bande de fréquences	**Puissance maximale à l'intérieur d'un bâtiment**	**Puissance maximale pour utilisation en extérieur**
2400-2454 MHz	100 mW	100 mW
2454-2483,5 MHz	100 mW	10 mW
5150-5250 MHz	200 mW	impossible
5250-5350 MHz	200 mW avec DFS/TPC ou equivalent ou 100mW avec DFS uniquement	impossible
5470-5725 MHz	impossible	impossible

source ART

*DFS : Dynamic Frequency Solution ; TPC :Transmit Power Control.

9.1.2.3. Les organismes de normalisation :

Deux organismes s'occupent de la standardisation des réseaux sans fil WLAN :

- ETSI :

En Europe, le groupe HiperLan (High Performance Radio LAN) issu de l'ETSI (European Télécommunications Standards Institut) définit deux standards, HiperLan 1 offrant un débit de 10 et 20 Mbit/s et HiperLan 2 offrant un débit de 54 Mbit/s.

- IEEE :

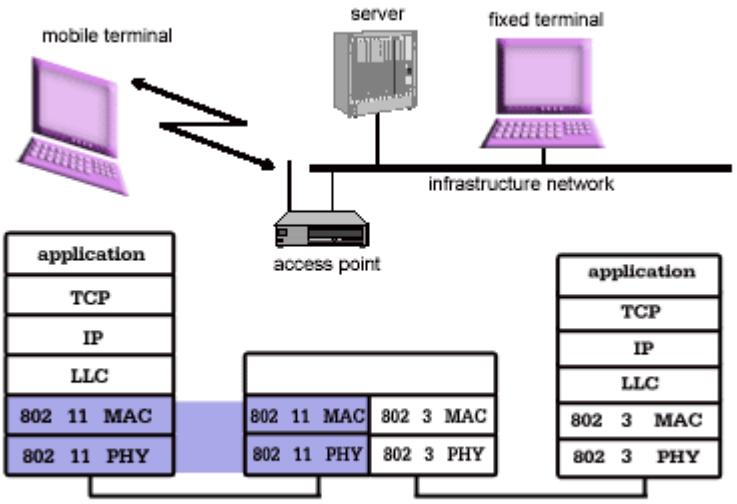
Au Etats-Unis c'est le comité 802 (dénommé ainsi par sa date de création : février 1980) issu de l'IEEE (Institut of Electrical and Electronics Engineers) qui a définit le standard IEEE 802.11 et ses extensions (802.11b, 802.11a…).
Ces deux standards sont incompatibles, de plus HiperLan utilise uniquement la bande U-NII tandis 802.11 utilise les bandes ISM et U-NII. A l'heure actuelle, seuls, des produits issus de la norme 802.11 sont commercialisés.

- WECA :

Le terme Wi-Fi (Wireless-Fidelity) est une norme délivrée par la WECA (Wireless Ethernet Compatibility Alliance) aux produits 802.11b. Cette dernière, composée de 140 entreprises, teste et gère l'interopérabilité entre les équipements répondant à la norme 802.11.b. Dernièrement le terme WIFI 5 certifie la norme 802.11a.

9.2. LE STANDARD IEEE 802.11

La norme 802.11, comme toutes les normes définies par le comité 802, couvre les deux premières couches du



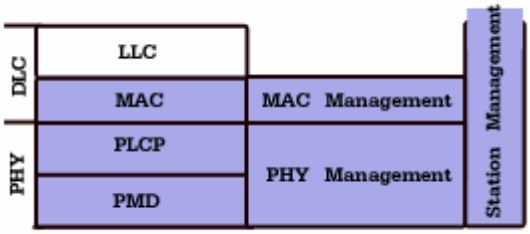
modèle OSI, c'est-à-dire la couche physique (niveau 1) et la couche liaison de données (niveau 2).

9.2.1. COUCHE 1 (802.11 PHY)

Généralités :

La couche physique définit la technique de transmission (modulation des ondes radioélectriques), l'encodage et la signalisation de la transmission. Le signal électrique hertzien va transporter l'information, il va être modifié suivant les informations à transporter (ici données binaires). Tout signal électrique sinusoïdal peut varier suivant son amplitude (tension en volt), sa fréquence (en hertz) et sa phase (en degré). C'est donc sur un de ces trois paramètres que l'on peut modifier un signal électrique pour le coder. On associe généralement modulation de fréquence et modulation de phase pour augmenter les performances.

La couche physique est divisée en deux sous couches. PLCP (Physical Layer Convergence Protocol) s'occupe de l'écoute du support et de la signalisation en fournissant un CCA (Clear Channel Assessment) à la couche MAC et PMD (Physical Medium Dependent) traite l'encodage des données et la modulation.

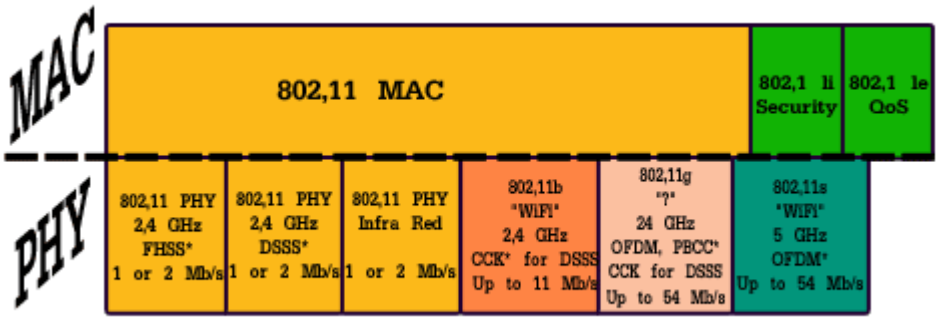


802.11 (Niv1) propose trois couches différentes suivant trois techniques de transmission (FHSS, DSSS, IR). De nouvelle techniques ont, depuis, été rajoutées : 802.11b (DSSS /CCK), 802.11a (OFDM), 802.11g (OFDM) pour les principales.

REMARQUE IMPORTANTE : les débits indiqués ne représentent pas les débits utiles mais les débits réels, nécessaires à une transmission radio fiable.

- 802.11 :

La norme physique 802.11 (ratifiée en 1997) propose deux types de transmission à modulation de fréquence



associés à une modulation de phase et une technique de transmission à infrarouge utilisée surtout en milieu industriel et très peu en informatique. Nous ne verrons que les deux types de transmission à modulation de fréquence qui utilisent plus précisément la technique à " étalement de spectre ". Cette technique, mise au point par des militaires, a connu un essor considérable car elle a de bonnes performances contre le brouillage et permet de faire cohabiter plus facilement dans une même bande de fréquence plusieurs transmissions.

FHSS (Frequency Hopping Spread Spectrum)/GFSK (Gaussian Frequency Shift Keying) ou étalement du spectre par saut de fréquence. On modifie la fréquence de la porteuse par une séquence de sauts. C'est-à-dire que l'émetteur change de fréquence d'émission de façon périodique et suivant une séquence préétablie, il synchronise le récepteur grâce à des trames balises qui contiennent la séquence de saut et la durée. Dans la norme 802.11 la bande de fréquence ISM définie de 2,400 à 2,4835 GHz est divisée en 79 canaux de 1 MHz et le saut se fait toutes les 300 à 400 ms. L'émetteur et le récepteur s'accordent sur une séquence de saut. La norme définit trois ensembles de 26 séquences possibles (78 séquences au total). Les signaux (données transformées par FHSS) sont ensuite modulés par une modulation de phase de type GFSK. Les débits atteignent 1 à 2 Mbits/s. Au départ cette technique était utilisée à des fins militaires afin de crypter la transmission mais les séquences de fréquences étant aujourd'hui standardisées, donc divulguées, la norme 802.11 l'utilise pour

remédier au phénomène d'interférences. De plus la norme Bluetooth utilise cette technique mais avec des séquences de saut différentes.
DSSS (Direct Sequence Spread Spectrum) ou étalement du spectre par séquence directe. De même que pour le FSSS, le DSSS est une technique dite à étalement de spectre fonctionnant sur la bande ISM des 2,4 GHz. Cette fois-ci la bande est divisée en 14 canaux de 20 MHz, chaque canal de 20 MHz étant constitué de quatre unités de 5 MHz. Chaque canal est espacé de 5 MHz, sauf le canal 14, espacé de 12 MHz avec le canal 13.
La largeur de bande étant de 83,5 MHz, on ne peut placer bout à bout 14 canaux de 20 MHz sans les faire se chevaucher. Lorsqu'un canal est sélectionné, le spectre du signal occupe une bande de 10 MHz de chaque côté de la fréquence crête, c'est pour cela qu'on ne peut utiliser que trois canaux distincts (donc trois réseaux) émettant sur une même cellule sans risque d'interférences.
Exemples d'association de trois canaux :
Il est essentiel d'affecter, à chaque point d'accès, des canaux qui ne se recouvrent pas. L'inconvénient majeur du DSSS est qu'il génère des pertes du à ces chevauchements. Une technique appelée " chipping " permet de résoudre ces pertes d'informations. Cette technique consiste à coder chaque bit en une séquence de 11 bits (appelé séquence Baker) :10110111000 lorsque le bit est à 1 et son complémentaire 01001000111 lorsqu'il est à 0. Cela permet d'effectuer des contrôles d'erreurs. Cette séquence ou signal, appelé " symbole ", est transmise à une vitesse de 1 MS/s (million de symboles par seconde). Le débit final en bit/s va être déterminé suivant la modulation de phase appliquée :

- BPSK (Binary Phase Shift Keying): ce type de modulation va encoder un bit à chaque changement de phase ? débit de 1Mbit/s.
- - QPSK (Quadrature Phase Shift Keying) : va encoder deux bits par changement de phase ? débit de 2 Mbit/s.
  Utilisation des canaux suivant les pays :

Pays	Etats-Unis	Europe	Japon	France
CANAUX UTILISES	1 à 11	1 à 13	1 à 14	1 à 13

- 802.11b (Wi-Fi)

Le comité IEEE a défini en 1999 une nouvelle couche physique, 802.11b ou 802.11HR (High Rate), permettant d'atteindre des débits de 5,5 à 11 Mbits/s. Cette nouvelle couche physique, dénommé Wi-FI par le WECA, s'implémente sur le standard 802.11. Cette norme utilise toujours la bande ISM et une modulation DSSS, ce qui la rend entièrement compatible avec 802.11 DSSS par contre le codage n'est plus à base de séquence Baker, mais un codage CCK (Complementary Code Keying) . On utilise aussi un mécanisme de modulation de phase QPSK mais à une vitesse de 1,375 MS/s, ce qui lui permet d'atteindre des débits de 11 Mbits/s. De plus un mécanisme d'adaptation environnemental permet de régler automatiquement le débit (Variable Rate Shiting) en fonction des conditions de réception (interférences, portée du matériel …).

Débit/Portée :

Vitesse	Portée		
	Aire ouverte	Aire semi-ouverte	Bureau fermé
11Mbps	160m	50m	25m
5.5Mbps	270m	70m	35m
2Mbps	400m	90m	40m
1Mbps	550m	115m	50m

Type de codage et modulation de phase :

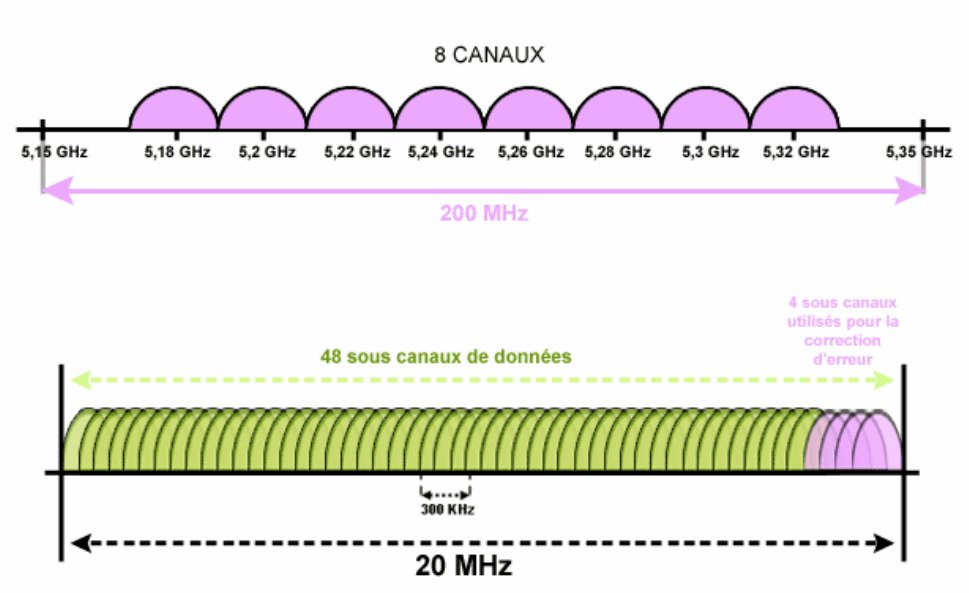
- 802.11a :

En parallèle à la norme précédente, en 1999 l'IEEE a finalisé une nouvelle couche physique: 802.11a. Dénommée Wi-Fi 5 par le WECA, cette couche physique utilise la bande radio U-NII des 5GHz, qui offre une largeur de bande plus importante (300MHz) et qui est beaucoup moins encombrée que la bande ISM. Par contre, elle est totalement incompatible avec les autres normes physiques. De plus la modulation de fréquence utilisée, OFDM (Orthogonal Frequency Division Multiplexing) est différente des autres normes physiques. On a constaté que plus les trames sont longues plus le chevauchement, dû aux interférences, inter trame est moindre. Cela démontre que plusieurs canaux à faible débit sont plus efficaces qu'un seul à haut débit.

Spécification des débits du 802.11 HR

Débit	Longueur du code	Modulation	Débit (symboles)	Nbre de bits/symbole
1 Mbit/s	11 bits (Barker Sequence)	PSK 1	1 MSps	1
2 Mbit/s	11 bits (Barker Sequence)	QPSK	1 MSps	2
5,5 Mbit/s	8 bits (CCK)	QPSK	1,375 MSps	4
11 Mbit/s	8 bits (CCK)	QPSK	1,375 MSps	8

OFDM : les deux premières sous-bandes (Low et Middle) de la bande U-NII sont divisées en 8 canaux de 20 MHz. Chaque canal est ensuite divisé en 52 sous-canaux de 300 MHz, 48 pour la transmission de données et 4 pour la correction d'erreur appelé FEC (Forward Correction Error)
8 CANAUX



C'est la transmission en parallèle de plusieurs sous-canaux à faible débit qui va créer, en fait, un seul canal à haut débit. De plus on peut utiliser huit canaux disjoints, sans interférence, permettant à huit réseaux Wi-Fi 5 d'émettre simultanément, alors que Wi-Fi n'en supporte que trois. Par contre l'inconvénient d'OFDM est qu'il réclame davantage de puissance que les techniques d'étalement de spectre, ce qui vide plus rapidement les batteries des appareils mobiles. 802.11a offre des débits de 6 à 54 Mbits/s suivant la modulation de phase utilisée :

- BPSK permet d'atteindre un débit de 6Mbits/s
- 64QAM (64-level Quadrature Amplitude Modulation) permet un débit de 54 Mbit/s.

802.11a PHY Layer Characteristics

PHY Mode	Modulation	Bit rate Mbit/s
1	*BPSK1/2*	*6*
2	*BPSK3/4 **	*9*
3	*QPSK1/2*	*12*
4	*QPSK3/4 **	*18*
5	*16QAM1/2*	*24*
6	*16QAM3/4 **	*36*
7	*64QAM2/3**	*48*
8	*64QAM3/4**	*54*

*) Optional. Only data frames, not control frames are usually sent using the optional PHY modes.

De même que pour Wi-Fi, Wi-Fi 5 utilise le " Variable Rate Shifting " lorsque l'environnement se dégrade. Le débit passant de 54Mbit/s à 48 puis 36, 24, 12 et 6 Mbit/s pour finir. Il est à noter que la portée est inférieure aux normes utilisant la bande ISM, car plus la fréquence est élevée, plus la portée diminue.

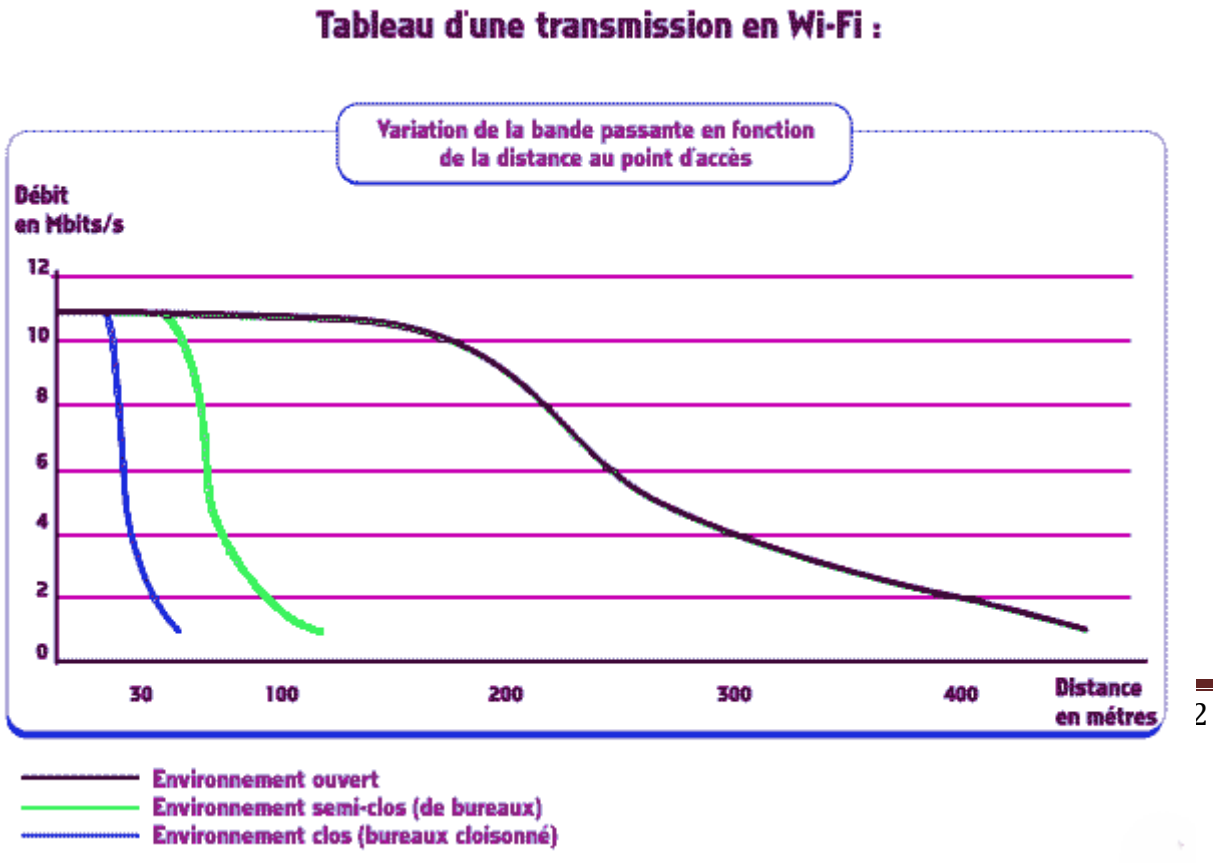
- 802.11g (validé en Juin 2003)

Dernière couche physique apportée au standard 802.11 et disponible depuis cette année mais pas encore ratifiée par la WECA. : 802.11g. Cette norme utilise la bande ISM comme Wi-Fi ainsi que la technique de codage CCK, ce qui la rend compatible avec Wi-Fi. Par contre elle utilise OFMD comme technique de transmission, ce qui lui permet d'atteindre un débit max de 54Mbits/s mais avec une consommation d'énergie plus importante. Les produits utilisant la norme 802.11g vendus sur le marché devrait proposer une compatibilité totale avec 802.11b.

Phénomènes physique (altération du signal / Solutions)

Le phénomène de propagation est un élément déterminant dans la transmission radio. Suivant le type d'environnement, les caractéristiques d'émission et de réception vont être profondément modifiées. En propagation directe, le signal reçu va décroître de façon linéaire, tandis qu'en milieu confiné, le signal reçu subit des modifications lors de son trajet. Il peut être atténué, diffracté, et également réfléchi. En règle générale on considère qu'il y a quatre chemins créés lorsqu'un signal subit une altération : le trajet direct, le trajet avec réflexion sur le sol, et deux trajets avec réflexion sur le mur. Deux autres éléments modifiant le signal pendant la transmission sont à prendre en considération : le déplacement de personnes, le changement de topologie physique (ouverture de portes …) et l'utilisation d'appareil tel que ventilateurs, four à micro onde…

Tableau d'une transmission en Wi-Fi :



Ce sont ces conditions de propagation qui vont déterminer toutes les conditions d'utilisation (vitesse de transmission et débit). Nous allons voir à présent en fonction de ces phénomènes d'altération, les techniques qui permettent à un signal électrique radio de mieux transporter l'information.
Fading :
Le signal radio lors de son trajet, subit, comme nous l'avons vu précédemment, des altérations et en particulier un appauvrissement appelé " fading " en anglais.
Contre ce phénomène on utilise une technique appelée " diversité ". Ce processus consiste à recueillir plusieurs transmissions du même message. Plusieurs types de diversités existent :

- La diversité spatiale (ou diversité d'antenne) est la plus utilisée :
- Le récepteur dispose de plusieurs antennes (minimum deux). Pour information, la longueur entre les antennes doit être un multiple de la demi-longueur d'onde de la fréquence de la porteuse. A la réception d'une trame il peut choisir la meilleure réception reçue par ses antennes, il peut aussi additionner ou combiner les signaux, ce qui améliore très sensiblement le résultat.
- -La diversité en fréquence, consiste à envoyer une trame sous différentes fréquences et on choisit la meilleure, ceci nécessite d'avoir un spectre de fréquence assez large.
- -Le fonctionnement de la diversité temporelle impose un temps d'attente entre deux trames (de l'ordre de 50 ms) ce qui affaiblit les performances du réseau.

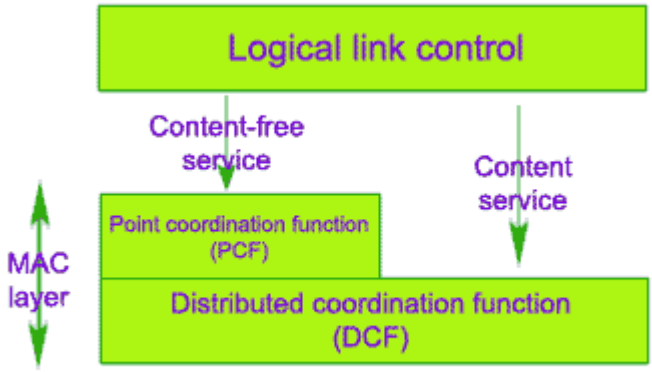
Trajets multiples :
Lors de l'envoi d'une trame, le récepteur reçoit cette trame en plusieurs exemplaires suivant les différents chemins possibles empruntés par la trame. La durée de réception est supérieure à son envoi car la trame d'origine et les échos produits se superposent. On calcule un delta (écart type du délai de propagation) s'il est supérieur de 10% à la durée de la trame on doit mettre en place des techniques de luttes contre ces interférences. Différentes techniques :

- Equalisation : On effectue une correction numérique de la transmission, on calibre cette correction en envoyant une trame d'apprentissage connue du récepteur. Le récepteur échantillonne le signal d'apprentissage prélevé sur une ligne de retard ce qui permet à l'équaliseur de régler son traitement numérique. Ce traitement sera ensuite appliqué à toutes les trames.
- -Etalement du spectre : Cette technique très différente de la précédente, est très développée dans la norme 802.11 car elle est utilisable dans des bandes de fréquences où d'autres transmissions coexistent. Les principales familles ont décrites précédemment.

9.2.2. COUCHE 2 (802.11 MAC)

- Généralités :

Au niveau 2, la couche liaison de données est subdivisée en deux sous couches : LLC et MAC. La sous-couche LLC, définie par la norme 802.11, est identique à la couche 802.2 permettant une compatibilité avec n'importe quel autre réseau 802, tandis que la sous-couche MAC est redéfinie par la norme 802.11 (Niv2). Elle caractérise l'accès au média de façon commune aux différentes normes 802.11 physiques, elle est équivalente à la norme 802.3 Ethernet avec des fonctionnalités nécessaires aux transmissions radio (le taux d'erreur est supérieur au support filaire) qui sont normalement confiées aux protocoles supérieurs, comme la fragmentation, le contrôle d'erreur (CRC), les retransmissions de paquet et les accusés de réception. De plus la couche MAC définit deux méthodes d'accès différentes, la Distributed Coordination Function (DCF) ou CP (Contention Period), appelée aussi mode d'accès à compétition, et la Point Coordination Function (PCF) ou CFP (Contention Free Period) appelée mode d'accès contrôlé. La méthode DCF est similaire à Ethernet permettant le transport des données asynchrones où les stations ont une chance égale d'accéder au support. La seconde méthode est le PCF, fondée sur l'interrogation à tour de rôle des stations, ou polling, contrôlée par le point d'accès. Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données. La méthode DCF est utilisée par les modes architecturaux Ad-Hoc et infrastructure, tandis que la méthode PCF n'est utilisée que par le mode infrastructure.



- Historique :

Historiquement il y a deux grandes familles, les protocoles à accès contrôlé et les protocoles à compétition : les premiers fonctionnaient sur le multiplexage temporel. Chaque hôte possède une partie de la communication disponible, il y a réservation de la bande passante. De nombreux inconvénients sont inhérents à cette technologie : réseau fermé, difficulté de gestion, peu performant, nombre de machine limitées. Le protocole Aloha, premier protocole à compétition est basé sur un accès partagé du support avec risque de collisions entre stations. Ne pouvant empêcher les collisions, il utilise un protocole de couche supérieure en mode connecté pour permettre la réémission de la trame. De plus pour éviter que la collision ne se reproduise, les stations ayant provoquées la collision, réémettent suivant un temps aléatoire. Ce protocole a permis le développement rapide des réseaux locaux. Mais comme il ne permet pas d'obtenir des performances satisfaisantes sur des réseaux de taille plus grande, il a été amélioré par l'ajout d'une détection de porteuse. Une machine peut écouter le bus pour savoir s'il y a une émission en cours, le nombre de collisions est considérablement diminué. C'est le CSMA (Carrier Sense Multiple Acces).

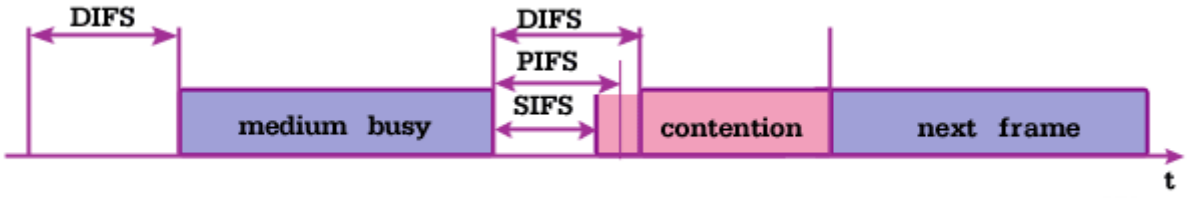
- 1970s: ALOHA
- 1972: Slotted ALOHA
- 1975: Carrier Sense Multiple Access (CSMA)
  - non persistent
  - p-persistent
- CSMA with collision detections (CD): Ethernet (1976)
- CSMA w/ coll. avoidance (CA): **IEEE 802.11 (1997)**

- De CSMA/CD à CSMA/CA :

Les machines utilisant le protocole CSMA savent si la ligne est occupée, mais si au même instant deux machines émettent il y a collision. Ces collisions doivent être détectées pour que la couche MAC puisse retransmettre sans passer par une couche supérieure. Un système a été rajouté au protocole, permettant aux machines d'écouter la ligne pendant qu'elles émettent, c'est la détection de collision (CD : Collision Detection). Le protocole de type CSMA /CD le plus utilisé s'appelle Ethernet. Ce système ne peut être implanté dans un environnement radio pour deux raisons : les liaisons radio utilisées ne sont pas full-duplex (on ne peut écouter et émettre en même temps) et une machine qui écoute la porteuse n'est pas certaine d'écouter toutes les stations connectées au point d'accès (cas de la station cachée). On a donc modifié le CSMA/CD pour arriver au CSMA/CA (Collision Avoidance) appelé protocole à évitement de collision.
DCF (mode CSMA/CA)
Le protocole CSMA/CA utilise plusieurs techniques pour palier à cette impossibilité d'écoute en émission. Tout d'abord un système d'accès au support basé sur des temporisateurs, un système d'acquittement positif, une gestion de reprise sur collision par des timers et une technique optionnelle permettant de sécuriser la transmission des données et d'éviter les collisions avec les nœuds cachés.

- L'accès au support :

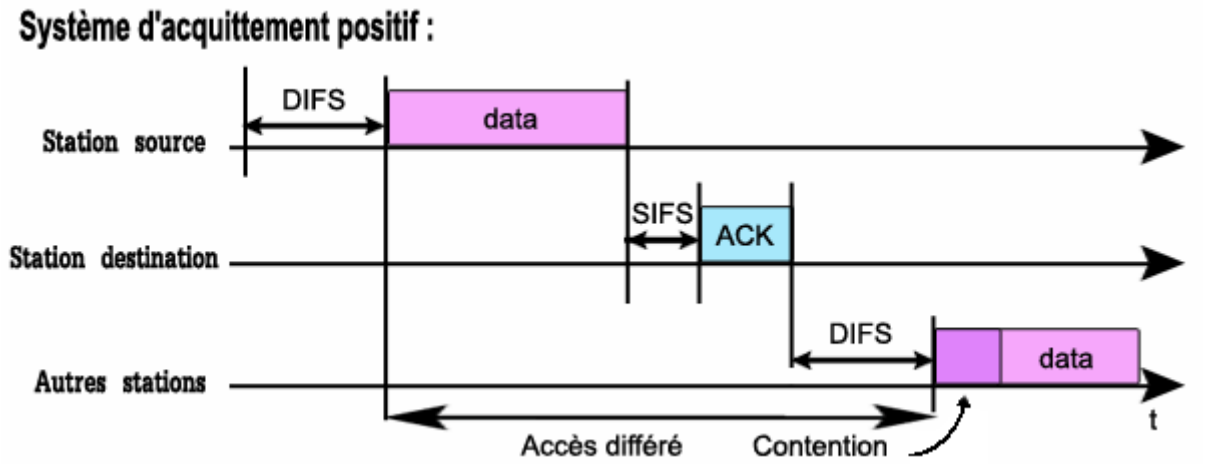
Chaque trame est délimitée par un espace. Cet espace permet la gestion d'accès au support en temporisant l'envoi de trames. Par le type de temporisateurs utilisés, on définit la priorité d'accès. Plus l'IFS (Inter Frame Space) est court plus l'accès est prioritaire. Il existe trois types d'inter trames différents :



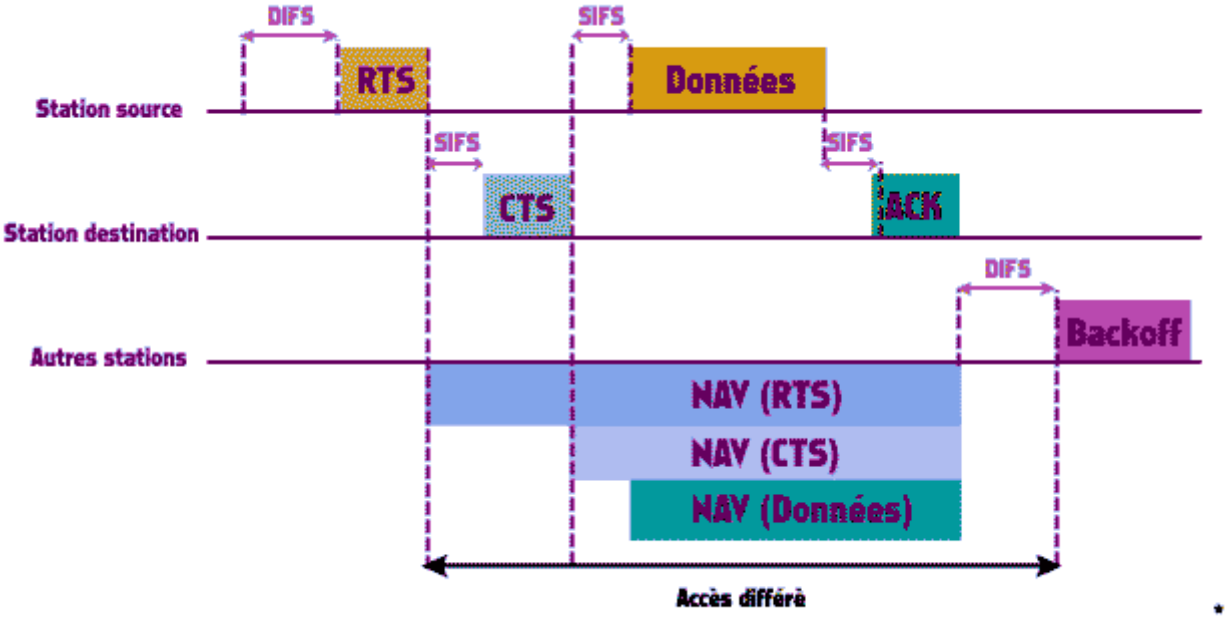
- SIFS (Short IFS) le plus petit des IFS, donc le plus prioritaire. Il est utilisé pour la transmission d'un même dialogue (données, ACK,…) accusé de réception de la station réceptrice et données de la station émettrice restent prioritaires.
- PIFS (PCF IFS) espace inter trame utilisé pour les trames PCF (accès contrôlé) par le point d'accès. Permet un accès prioritaire de ce PA sur les stations du réseau. Sa valeur correspond à un SIFS plus un temps (time slot).
- -DIFS (DCF IFS) temporisateur inter trame pour l'accès distribué utilisé par les stations pour accéder au support (en mode DCF).
- Remarque : Le fait que les inters trames PIFS soient plus courtes que les inters trames DIFS montrent bien que les données envoyées dans le mode PCF sont prioritaires sur les données envoyées en mode DCF.
- VALEURS DES ESPACES (en fonction de la couche physique) :

	FHSS	DSSS
Timeslot (µs)	50	20
SIFS (µs)	28	10
DIFS (µs)	128	50
PIFS (µs)	78	30

- Système d'acquittement positif :



Lorsqu'une station veut émettre des données, elle écoute le support. Si le support est libre pendant un DIFS, la station émet, si par contre elle détecte une transmission, elle utilise un timer appelé NAV (Network Allocation Vector), lui permettant de suspendre ses transmissions. Ce NAV s'applique à toutes les stations et elles n'ont la capacité d'émettre qu'après la fin du NAV. Le NAV est calculé par rapport au champ TTL (Time To Live) des trames envoyées. Cela permet aux stations situées dans le voisinage des stations source et destination de connaître la durée du cycle complet de la transmission à venir. Ces différentes stations en attente d'émission risquent de créer de collisions si on n'utilise pas une technique de gestion lorsque le support sera à nouveau libre. Ce procédé de redémarrage s'appelle l'algorithme de backoff, chaque station calcule un délai aléatoire compris entre 0 et 7 " time slot " (unité de temps la plus petite, variant suivant la norme physique) et décrémente ce timer dès que le support est libre. La station atteignant la valeur 0 la première pourra transmettre ses informations, les autres bloquent leur temporisateur et recommencent dès que le support est de nouveau libre. Si deux stations ont la même valeur de timer une collision se produira. Ces stations devront régénérer alors un nouveau compteur, compris cette fois entre 0 et 15. Cet algorithme permet aux stations d'accéder au support avec la même probabilité, mais sans garanti de délai.



Technique de sécurisation de transmission par réservation (option):
L'écoute du support se fait au niveau de la couche physique avec le PCS (Physical Carrier Sense) et au niveau de la sous couche MAC, avec le VCS (Virtual Carrier Sense). Le PCS détecte l'occupation du canal en analysant les trames passant sur le support hertzien, le VCS est un mécanisme de réservation basé sur l'emploi de trames RTS / CTS (Request To Send / Clear To Send) entre hôte source et hôte destination. Son fonctionnement est

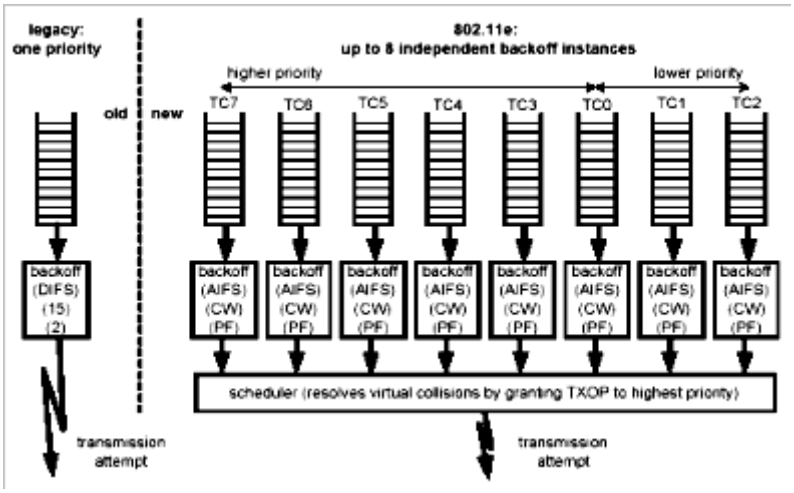
simple : une station désirant émettre envoie un RTS, les stations du BSS lisent ce RTS et initialisent leur NAV en fonction des paramètres contenu dans ce RTS. La station destination répond, après un SIFS, par un CTS, de nouveau les autres stations mettent à jour leur NAV en fonction de ce CTS. La station source, ayant reçu ce CTS, est assurée que le support est réservé pour sa transmission. Cette méthode est optionnelle et plutôt utilisée pour l'envoi de grosses trames qui feraient chuter les performances en bande passante si il y a collisions. On peut justement calculer un seuil permettant d'utiliser ou non le mécanisme RTS /CTS (RTS Threshold). Une deuxième application, très utile pour l'univers des liaisons radio, est la détection des stations cachées. Deux stations d'un .même BSS peuvent être hors de portée radio l'une de l'autre tout en étant sur le même PA. Si elles veulent émettre en même temps il va y avoir collision. Par contre s'il y a réservation avant transmission par la fonction RTS/CTS les stations cachées de la station source, vont quand même détecter le CTS du point d'accès. Il est à noter que des collisions peuvent se produire entre trames RTS, mais de part leur petite taille, la bande passante n'est pas trop affectée.
Le protocole CSMA/CA permet de gérer les collisions tout en palliant aux contraintes dues aux transmissions radio. Par contre les mécanismes mis en place alourdissent les échanges (trames spécifiques wifi) ce qui rend les performances plus faible qu'un réseau filaire.

PCF (mode d'accès centralisé) :
La norme 802.11 prévoit une possibilité de réservation de canal permettant d'utiliser des services à temps réel. Ce système permet de mettre en œuvre un accès contrôlé de type réservation. Ce contrôle est opéré uniquement par un point d'accès (PA), qui va, suivant un multiplexage temporel, organiser une scrutation successive des stations (polling). Dans ce mode ce ne sont plus les stations qui essaient d'accéder au support mais le point d'accès qui contrôle le support. Celui-ci choisit la station qui pourra transmettre. Le mode PCF est optionnel dans la norme 802.11, il est toujours utilisé en alternance avec le mode DCF qui est toujours le mode d'accès principal. D'ailleurs une station peut utiliser ces deux modes à la fois. C'est lors du processus d'association que le point d'accès et la station indiquent s'ils implémentent cette fonction. L'activation se fait pour le point d'accès (PA), au travers de certains champs de trames de type balise, réponse d'association et pour la station associée, au niveau des trames de requête d'association et requête de vérification. Le point d'accès établi une liste d'interrogation (polling list) des stations associées fonctionnant en mode PCF. Le point d'accès peut gérer des stations fonctionnant dans les deux modes. Le mode PCF s'organise autour d'une " super trame " découpée en deux parties : une partie où le mode PCF est activé, c'est la CFP (Contention Free Period) qui correspond à une période de temps sans contention et une autre où l'on passe en mode classique DCF (accès distribué), c'est la CP (Contention Period) qui correspond à une période de temps avec contention. Le PA génère une balise, appelée Beacon Frame, pour indiquer le passage en mode PCF, après une inter trame PIFS. Cette balise est de type DTIM (Delivery Traffic Information Map) puis la station coordinatrice (PA) va interroger chaque station par des trames de type CF.Poll (Cotention Free Polling). La station interrogée peut alors transmettre ses données, à la fin le PA reprend la main et interroge la station suivante de la liste d'interrogation. Le mode PCF correspond à une qualité de service (QOS) pour le 802.11 mais cette fonction n'est pas implantée dans la plupart des équipements. Un standard traitant de la qualité de service à part entière va apparaître avec la norme 802.11^{e}
Sous Normes 802.11 MAC :

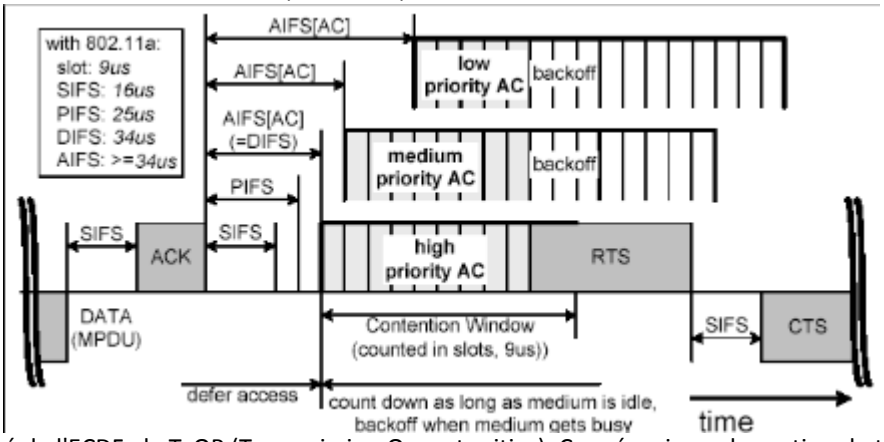
- 802.11e (QoS)

La méthode d'accès PCF n'a jamais été utilisée car aucun constructeur ne l'a implémentée dans des produits. Le groupe IEEE 802.11e a pour but d'améliorer la QoS (Quality of Service) dans les deux modes, DCF et PCF.en ajoutant deux nouvelles méthodes d'accès, EDCF (Extended DCF) et HCF (Hybrid Coordination Fonction).

EDCF : aujourd'hui les trames wifi ont la même priorité quelque soit la station émettrice. EDCF définit huit catégories de trafic (TC :Traffic Categories) donc huit niveaux de priorités. Chaque station en mode EDCF gère



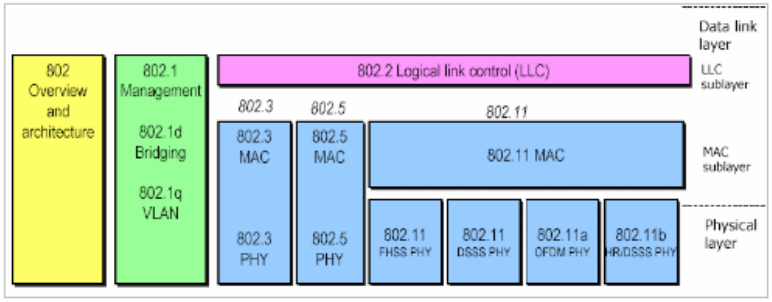
huit files d'attentes pour chaque type de trafic.
Ces huit catégories de trafic possèdent leurs propres paramètres de temporisateurs (IFS, Backoff). De plus les valeurs des temporisateurs ne sont plus fixes. On conserve les ISF du mode DCF auquel on ajoute un nouveau temporisateur, l'AIFS (Arbritration IFS). Cet AIFS correspond au DIFS mais sa valeur est variable en fonction du niveau de priorité de la station émettrice (AIFS=DIFS)

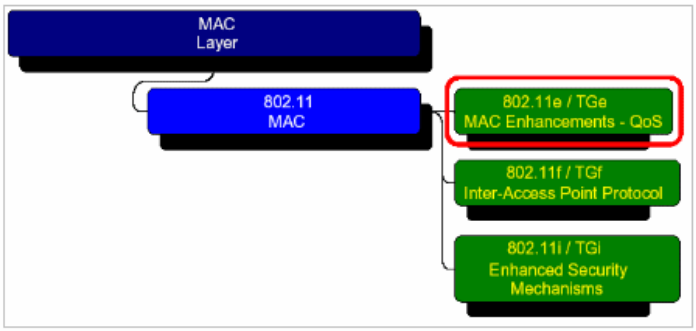


Autre nouveauté de l'ECDF : le TxOP (Transmission Opportunities). Ce mécanisme de gestion de transmission définit le droit d'accès d'une station et son temps alloué en fonction de son niveau de priorité. Si plusieurs stations de catégories de trafics différents accèdent au support en même temps, le TxOP, qui est un temps prédéterminé (catégorie de trafic la plus haute? temps le plus court), donnera l'accès à la catégorie la plus prioritaire. Ce temporisateur s'ajoute à la fin du temporisateur de backoff
HCF : cette deuxième méthode, comme pour le PCF, utilise le point d'accès pour gérer le trafic en définissant des périodes avec et sans contention (CP et CFP), d'où le terme d'hybride.
802.11f : voir " Gestion de la mobilité (roaming) "
802.11h :
Cette norme vise à rendre compatible les équipements 802.11a avec les infrastructures Hiperlan2. Adoption des technologies DFS (Dynamic Frequency Solution) et TPC (Transmit Power Control) pour se conformer aux normes européennes. Ce qui permet l'assignation automatique des fréquences et du contrôle automatique de la puissance d'émission pour éviter les interférences entre les points d'accès.
802.11i : Voir " SOLUTIONS INTERNES FUTURES "
802.11j :

Convergence du standard américain 802.11a et européen Hiperlan.

TABLEAU RESUMANT LES NORMES 802.11





9.3. ARCHITECTURE

9.3.1. ARCHITECTURE DU MATERIEL

9.3.1.1. Deux modes :

- Infrastructure :
- Le mode infrastructure se base sur une station spéciale appelée Point d'Accès (PA). Ce mode permet à des stations wifi de se connecter à un réseau (généralement Ethernet) via un point d'accès. Elle permet à une station wifi de se connecter à une autre station wifi via leur PA commun. Une station wifi associée à un autre PA peut aussi s'interconnecter. L'ensemble des stations à portée radio du PA forme un BSS (Basic Service Set). Chaque BBS est identifié par un BSSID (BSS Identifier) de 6 octets qui correspond à l'adresse MAC du PA.

  Ad-Hoc :

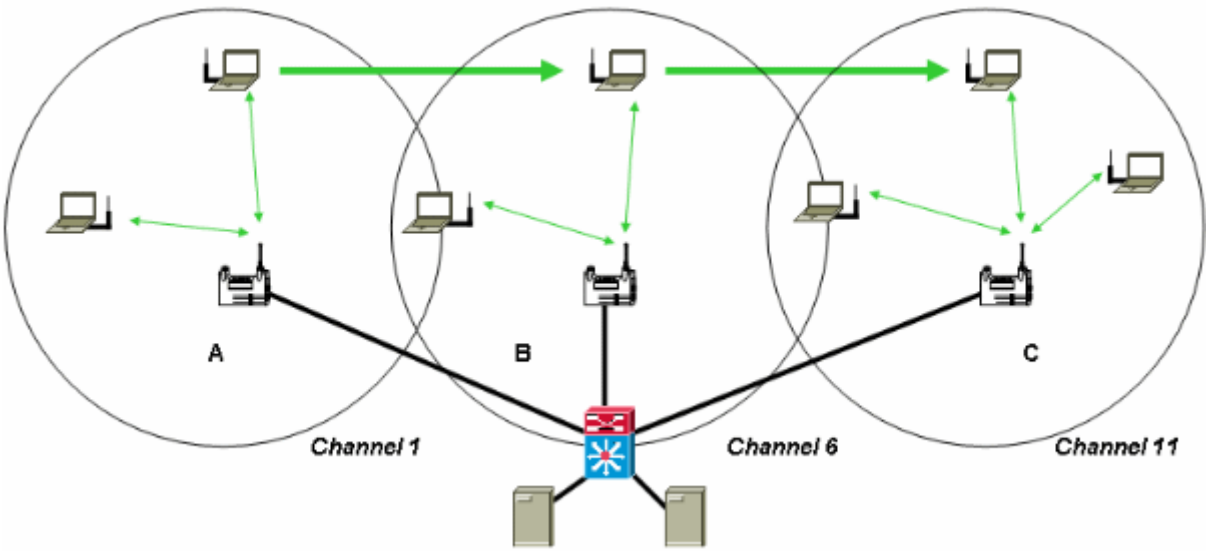
Le fonctionnement de ce mode est totalement distribué, il n'y a pas d'élément structurant hiérarchiquement la cellule ou permettant de transmettre les trames d'une station à une autre. Ce mode permet la communication entre deux machines sans l'aide d'une infrastructure. Les stations se trouvant à portée de radio forment un IBSS (Independant Basic Service Set).

9.3.1.2. Interconnexion :

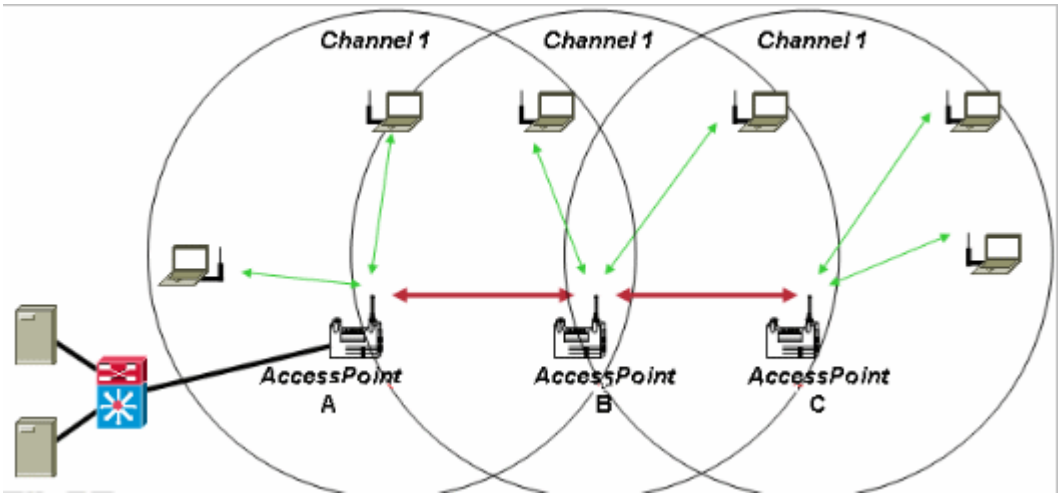
On peut composer un réseau avec plusieurs BSS. Ceux-ci sont reliés entre eux par un système de distribution (DS) connecté à leurs points d'accès. Ce DS est généralement le réseau Ethernet sur lequel le PA se connecte mais il peut correspondre à du token ring, FDDI ou un autre réseau 802.11. Ces différents BSS interconnectés via un DS forme un ESS (Extended Service Set). Un ESS est identifié par un ESSID (abrégé en SSID) qui est constitué d'un mot de 32 caractères qui représente le nom du réseau.
On peut associer un IBSS au sein d'un ESS.

9.3.2. EXEMPLES D'ARCHITECTURES :

L'extension du BSS (même SSID) forme un ESS. La station peut se déplacer du point d'accès A au point d'accès C.

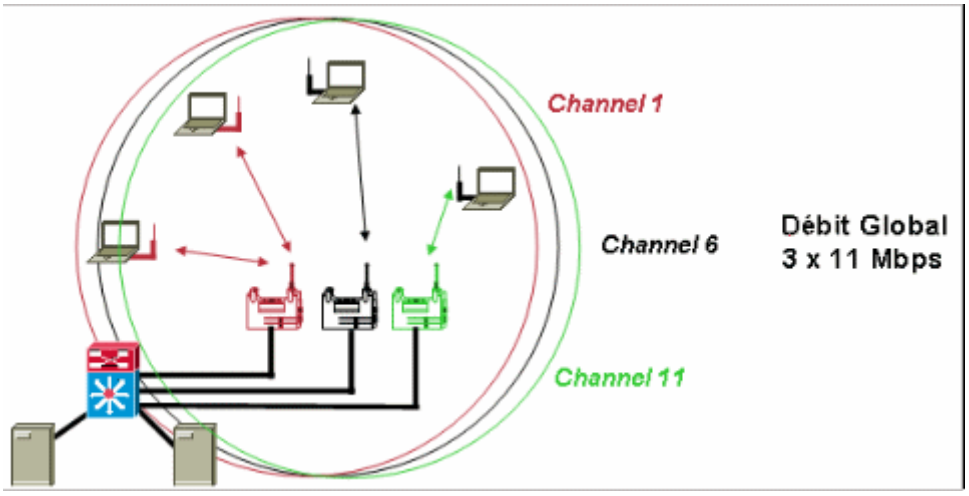


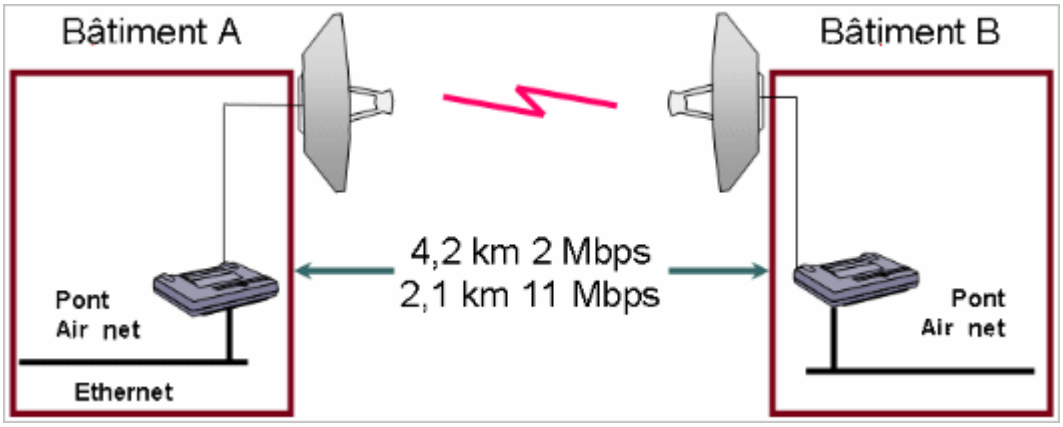
·Point d'accès en mode répéteur : permet d'étendre la zone de couverture du BSS, partage de la bande



passante totale sur toute la zone.

·Partage de charge : trois canaux recouvrent la même zone et augmentent ainsi le débit. La station détermine le meilleur point d'accès suivant le signal et la charge de l'AP.





·Interconnexion à distance de réseaux privés : ici la norme Wi-Fi permet d'interconnecter deux bâtiments.

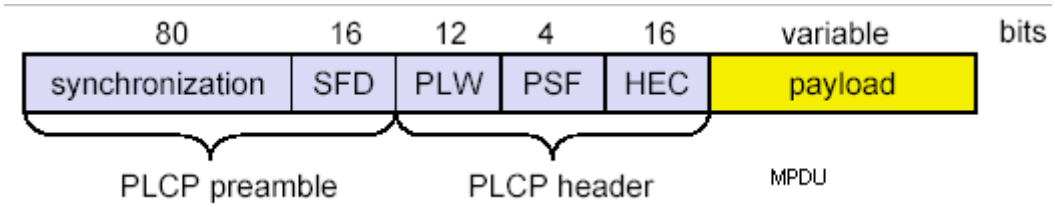
9.4. LES TRAMES

Les paquets de données, provenant de la couche réseau, sont encapsulés au niveau 2 par un en-tête MAC, formant une MPDU (Mac Protocol Data Unit). Cette MPDU est ensuite encapsulée dans une seconde trame au niveau 1 (physique) pour permettre la transmission sur le média. Cette encapsulation consiste à rajouter un préambule et un en-tête à la MPDU, cet ensemble forme une PLCP-PDU. Le préambule et l'en-tête différent suivant la couche physique utilisée. Nous allons voir les différentes trames du niveau physique (PLCP-PDU), puis celles du niveau liaison de données (MPDU).

9.4.1. NIVEAU PHYSIQUE

Le préambule permet la détection du début de trame, la synchronisation de la trame, il permet la prise du canal pour l'émission ou CCA (Clear Channel Assesment).
L'en-tête contient diverses informations, variable suivant l'interface physique utilisée.

9.4.1.1. TRAME FHSS (802.11 FHSS) :



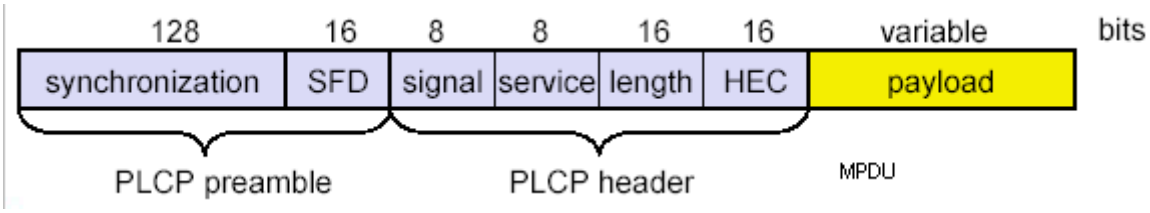
Préambule (preamble) en deux parties :

- 80 bits de synchronisation (alternance de 0 et de 1) permet de sélectionner le meilleur point d'accès et de se synchroniser avec (PA et STA).

- SFD (Start Frame Delimiter) de 16 bits (0000 1100 1011 1101): indique le début de la trame.
- En-tête (header) en trois parties :
  - PLW (PLCP-PDU Length Word) sur 12 bits: indique la longueur (en nombre d'octets) de la trame (PLCP-PDU), cela permet à la couche physique déterminer la fin de la trame.
  - PSF (PLCP Signaling Field) sur 4 bits: indique le débit utilisé sur l'interface radio. (1 ou 2 Mbits/s) pour la transmission des données (MPDU).
  - HEC (Header Error Check) est un CRC de 16 bits permettant de détecter les erreurs des champs de l'en-tête (PLW et PSF).

Remarque : le préambule et l'en-tête sont toujours transmis à 1 Mbits/s.

9.4.1.2. TRAME DSSS (802.11 DSSS ; 802.11b) :



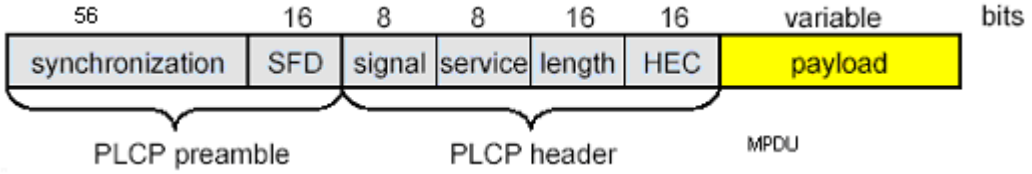
Préambule : identique à la trame FSSS, si ce n'est une longueur de synchronisation plus longue et une valeur de 0xF3A0 (1111 0011 1010 0000) pour le SFD.

En-tête en quatre parties :

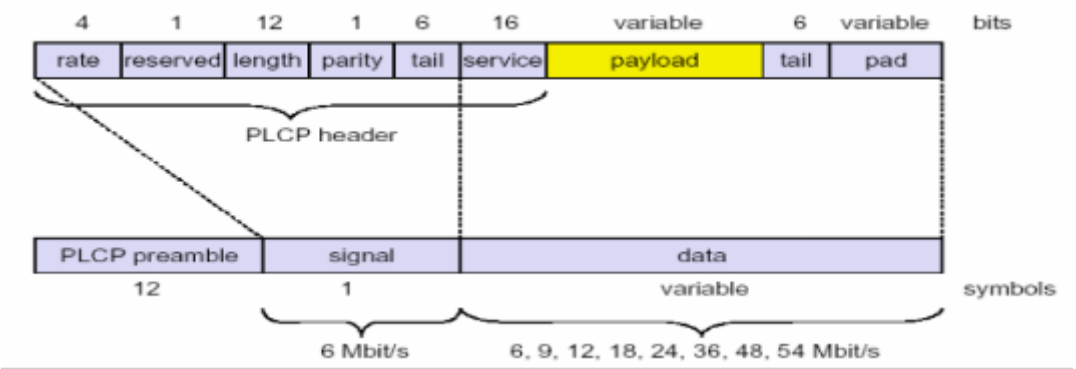
- Signal sur 8 bits : indique la vitesse sélectionnée pour la transmission des données (MPDU) :
  - 0x0A pour 802.11 en mode BPSK (1Mbits/s)
  - 0x14 pour 802.11 en mode QPSK (2Mbits/s)
  - 0x37 pour 802.11b en mode QPSK (5,5Mbits/s)
  - 0x6E pour 802.11b en mode QPSK (11Mbits/s)
- Service sur 8 bits : réservé pour un usage futur (valeur 0x00 ?IEEE802.11)
  - Lenght sur 16 bits : indique la longueur (en nombre d'octets) de la trame à suivre (MPDU), cela permet à la couche physique déterminer la fin de la trame.
  - HEC (Header Error Check) est un CRC de 16 bits permettant de détecter les erreurs des champs de l'en-tête (Signal, Service et Lenght).

  Remarque : le préambule et l'en-tête sont toujours transmis à 1 Mbits/s.

  De plus pour la norme 802.11b il existe un deuxième type d'encapsulation dont le préambule est plus court (72bits au lieu de 144bits) :



9.4.1.3. TRAME OFDM (802.11a, 802.11g):



Préambule : réalisé grâce à une séquence ce douze symboles permettant la détection du signal par le récepteur et le début de la trame.

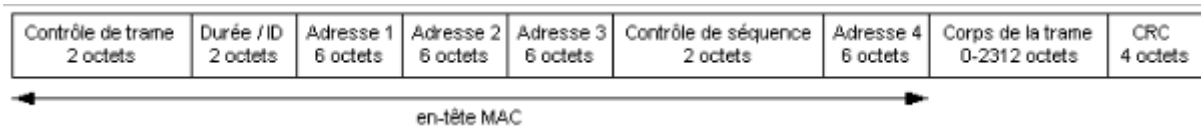
En-tête en six champs :

- -RATE : indique le débit de transmission
  - 1 bit réservé toujours à 0
  - Lenght : indique le nombre d'octets dans la trame.
  - 1 bit de parité des trois champs précédents
  - Tail (en-queue) : champs réservé, toujours à 0
  - Service : champ réservé, toujours à 0
- MPDU :
  - Tail : champ réservé, toujours à 0
  - Pad : champ de padding (remplissage) de 6 bits minimum permettant une structure se comptant en octets.

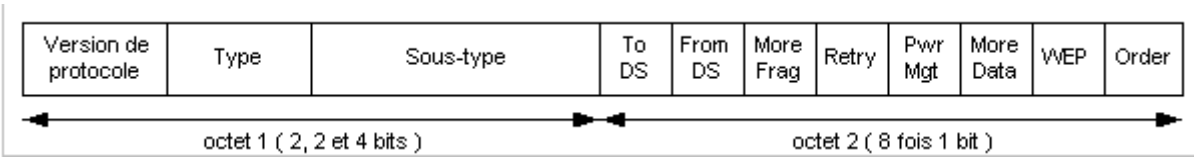
9.4.2. NIVEAU MAC

Il existe trois sortes de trames : les trames de données, les trames de contrôle utilisées pour l'accès au support (RTS, CTS, ACK…) et les trames de gestion utilisées pour l'association à un point d'accès ou pour la synchronisation et l'authentification. La représentation de la trame est une représentation générale et ses champs changent suivant la fonction de celle-ci. La taille maximale d'une trame est de 2347 octets.

9.4.2.1. FORMAT GENERAL.



EN-TÊTE (7 champs sur 30 octets): C'est la partie la plus complexe car elle intègre de nombreuses fonctions.



·Contrôle de trame (11 sous champs sur 2 octets):

- Version de protocole : toujours à 0 pour la version actuelle (2 bits)
- Type et sous type : représente les 3 sortes de trames et leurs fonctions (2+4 bits)
- To DS et From DS : DS=Distribution Service (point d'accès).
- To DS : (bit à 1) la trame est adressée au point d'accès pour qu'il l'a fasse suivre.
- From DS (bit à 1) la trame vient du point d'accès.
- More Fragments : à 1 si les données sont fragmentées, à 0 si elles ne sont pas fragmentées ou s'il s'agit du dernier fragment (1 bit).

Retry : à 1 s'il s'agit d'une retransmission (1 bit).
Power Management : à 1 si la station est en mode d'économie d'énergie, à 0 si elle est active (1 bit). Venant du point d'accès, les trames sont toujours en mode actif.
More Data : 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 (1 bit).
WEP : ce bit indique que le corps de la trame est chiffré suivant l'algorithme WEP.
Order : si à 1 cela indique que la trame est envoyée en utilisant une classe de service strictement ordonné. Ne permet pas à la station d'envoyer des trames en multicast.
Durée/ID (2 octets) :
Ce champ a 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 ou AID (Association IDentity)
- dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV.

·Champs adresses (4 fois 6 octets) :
L'adresse MAC de 48 bits se décompose en trois parties

- un groupe de 2 bits au début de adresse : le premier indique si l'adresse est individuelle (bit à1) ou de groupe (bit à 0), le deuxième indique si l'adresse est locale (bit à 1) ou universelle (bit à 0). Si l'adresse est locale, les 46 bits suivants sont définis localement.
- un groupe de 22 bits : numéro constructeur défini par l'IEEE
- un groupe de 24 bits : numéro de série défini par le constructeur

Adresses de groupe :

- adresse broadcast : définit l'ensemble des stations du réseau.(les 48 bits sont à 1)
- adresse multicast : définit un groupe de stations en nombre fini.

Types d'adresse :

La structure d'adressage 802.11 est plus riche que pour un réseau filaire. Car si on veut accéder à une station du même réseau (BSS), il faut passer par le point d'accès donc indiquer son adresse MAC pour qu'il relaie le paquet. De même pour accéder à une station d'un autre réseau (ESS), deux adresses intermédiaires peuvent être indiquées. Ces champs d'adresses sont définis en accord avec les indications des champs To DS et From DS. Nous allons voir les quatre types d'adresse :

- BSSID (Basic Service Set Identifier):
  - En mode infrastructure -> @ MAC du PA
  - En mode Ad-Hoc -> @ MAC locale du BSSID (générée lors de la création de l'IBSS).
- DA (Destination Address) : adresse, individuelle ou de groupe, identifie le(s) destinataire(s).
- SA (Source Address) : adresse individuelle ayant transmis la trame.
- RA (Receveir Address) : BSSID destination (point d'accès récepteur).

ToDS	FromDS	@1 destination Récepteur	@2 source Emetteur	@3 sce initiale dest finale	@4 WDS*	ETAPE
0	0	DA	SA	BSSID	---------	0
1	0	BSSID	SA	DA	---------	1
0	1	DA	BSSID	SA	---------	2
1	1	RA(BSSID)	TA(BSSID)	DA	SA	3

- TA (Transmitter Address) : BSSID source (point d'accès émetteur).

*Wireless Distribution Service (liaison entre deux PA)

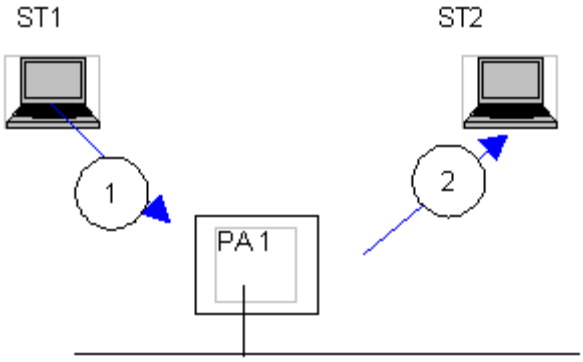
Exemple d'adressage:

Le mode Ad-Hoc : transmission dans un IBSS, ST1 envoie ses données vers ST2.

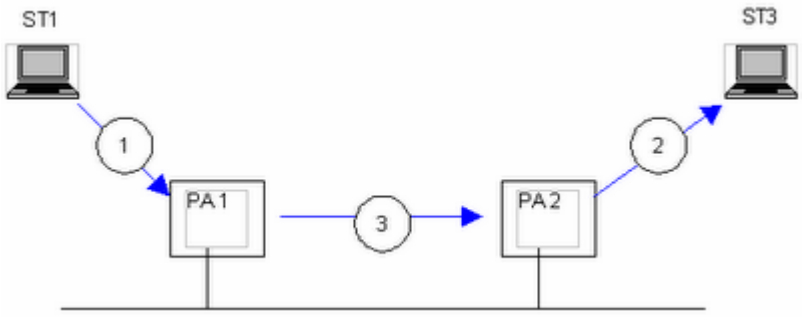
Etape 0: @1: ST1, @2: ST2, @3: BSSID de l'IBSS.

Le mode infrastructure :

-1er Cas : transmission dans un même BSS, ST1 envoie ses données vers ST2 (via PA1).



Etape 1 : ST1 envoie la trame vers PA1 pour destination finale ST2.
To DS: à 1, @1 : PA1 (dest); @2 : ST1 (sce), @3 :ST2 (dest finale).
Etape 2 : PA1 envoie la trame vers ST2.
From DS à 1, @1 : ST2 (dest), @2 : PA1, @3 : ST1 (sce initiale).
-2em Cas: transmission dans un même ESS, ST1 envoie ses données vers ST3 (via PA1 et PA2).



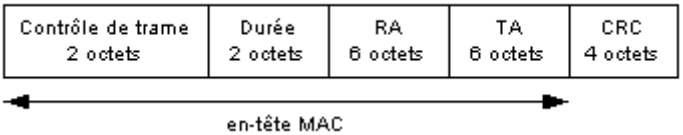
A la différence de l'exemple précédent, l'étape 3 suit l'étape 1.
Etape 3 :PA1 envoie la trame vers PA2
To DS et From DS sont à 1, @1 : PA2 (dest), @2 : PA1 (sce), @3 :ST3, @4 :ST1.
·Contrôle de séquence (2 octets) :

- numéro de séquence (12 bits) : numéro assigné à chaque trame.
- numéro de fragment (' bits) : numéro assigné à chaque fragment, si la trame est fragmentée.

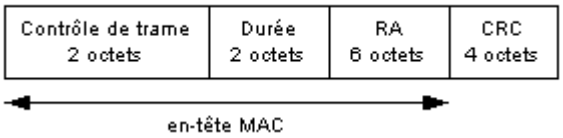
Corps de la trame (données) (0-2312 octets) : La taille peut être supérieure à 1500 octets à cause du chiffrement WEP. Il n'y a pas de données pour les trames de contrôle et de gestion.
·FCS (Frame Check Sequence) (4 octets) : CRC de 32 bits, pour le contrôle d'intégrité de la trame.

9.4.2.2. FORMAT TRAME DE CONTROLE :

Les trames de contrôle permettent l'accès au support et ont pour fonction d'envoyer les commandes et informations de supervision aux éléments du réseau. Dans la partie contrôle de trame, les champs de " ToDS " à " order " sont à 0.
Trames principales :
RTS (Request to send) est utilisé pour réclamer le droit de transmettre une trame de données

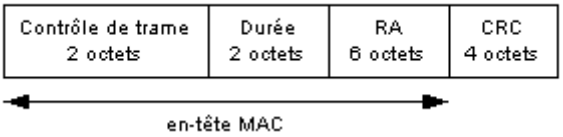


- RA est l'adresse du récepteur destinataire de la prochaine trame de données ou de gestion.
- TA est l'adresse de la station qui transmet la trame RTS.
- CTS (Clear To Send) correspond à la réservation du canal pour émettre une trame de données



- RA correspond à l'adresse de la station source (champ TA) de la trame RTS.

ACK permet l'acquittement des trames de données



RA correspond à l'adresse de la station source, qui provient du champ adresse 2 de la trame de données ou de gestion précédente.

9.4.2.3. FORMAT TRAME DE GESTION :

Il existe quatre familles de trames de gestion :

- Trames liées aux fonctions d'association-désassociation
- Trames d'interrogation du voisinage radio
- Trames liées aux fonctions d'authentification
- Trames balises, utilisées par le point d'accès pour diffuser des informations dans le BSS, gestion du mode économie d'énergie grâce aux balises TIM et DTIM.

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

TABLEAU DES VALEURS (Types et Sous Types)

9.5. SECURITE

9.5.1. INTRODUCTION :

Le point crucial lors d'une installation réseau, quelle soit filaire ou sans fil, est la mise en place d'éléments de protection. La sécurité a toujours été le point faible des réseaux wifi, à cause principalement de sa nature physique : les ondes radio étant un support de transmission partagé quiconque se trouvant dans la zone de couverture peut écouter le support et s'introduire dans le réseau. On peut même, grâce à des antennes amplifiées, se trouver hors de portée de la couverture radio pour pénétrer ce réseau. Ces problèmes de sécurité se posent aussi pour des réseaux câblés mais l'écoute passive nécessite une intrusion physique. Car toute personne possédant quelques notions d'informatique et un peu de matériel peut facilement trouver les informations et les programmes pour écouter et percer des réseaux wifi. En plus de ces faiblesses intrinsèques aux ondes radio, un réseau wifi doit se protéger des attaques classiques. Ces failles de sécurité ont porté un préjudice certain à son développement en entreprise, car ces failles deviennent les points d'accès au réseau interne sur lequel il est connecté. Il existe des moyens de sécurité implantés de base sur le matériel wifi (carte et point d'accès) permettant un premier niveau de protection, mais ces moyens de sécurisation sont facilement contournable. De nouvelles parades de sécurité sont en cours de normalisation et seront utilisables d'ici quelques mois, pour l'instant le meilleur moyen de sécurisation est d'utiliser les mêmes mécanismes de protection que les réseaux filaires.
Nous allons tout d'abord, avant de voir les différentes attaques susceptibles d'atteindre un réseau wifi, revoir quelques notions utiliser qui répondent aux trois principes élémentaires de sécurité qui sont : Codage, Authentification et Intégrité.

9.5.2. QUELQUES NOTIONS :

9.5.2.1. LA CRYPTOGRAPHIE :

La cryptographie consiste à rendre un texte incompréhensible en le codant. On code (crypte ou chiffre) le texte en effectuant une opération sur le texte en clair à partir d'une règle appelée clé de chiffrement. Le texte codé (cryptogramme) peut alors être envoyé à son destinataire. La cryptanalyse consiste à déchiffrer un texte codé en effectuant sur ce texte avec une clé. Il existe trois méthodes de cryptographie : à clé symétrique, à clé asymétrique (ou clé publique), à clé mixte (utilisation des deux précédentes).
Remarque : en France la réglementation limite la longueur maximale de la clé à 40 bits pour un usage public et 128 bits pour un usage privé.
Clé symétrique :
L'expéditeur et le destinataire utilisent la même clé (pour le codage et le décodage), toutes les personnes voulant se transmettre des données doivent partager la même clé. Les algorithmes utilisant ce système sont rapides et fiables, par contre la faille de ce système réside dans la transmission de cette clé partagée. Types d'algorithmes à clé symétriques :

- DES (Data Encryption Standard) : a été le plus utilisé, mais n'est plus utilisé depuis 1998 considéré peu sûr. Clé de 40 à 56 bits.
- IDEA (International Data Encryption Algorithm) : est utilisé par PGP (Pretty Good Privacy), le logiciel de cryptographie le plus utilisé au monde. Clé de 128 bits.
- Série RC (Ron's Code) RC2 à RC 6 : algorithme développé par Ron Rivest, la version RC4 est utilisé dans le protocole WEP d'IEEE 802.11.
- AES (Advanced Encryption Standard) : remplaçant du DES dans l'administration américaine et du RC4 dans la norme 802.11 avec 802.11i. Fondé sur l'algorithme de Rijndael, est considéré comme étant incassable.

Clé asymétrique ou clé publique :
Ce système résout le problème de transmission des clés rencontré précédemment. En 1976, deux mathématiciens, Whitfield Diffie et Martin Hellman, ont proposé une nouvelle façon de chiffrer. On utilise deux clés, une clé privée pour déchiffrer les données, mais qui reste confidentielle, et une clé publique pour chiffrer les données, qui elle peut être transmise et laissée à la disposition de tous les utilisateurs. Principe de fonctionnement entre deux utilisateurs (A l'expéditeur et B le destinataire) :
1)B fabrique deux clés (P=publique, S=secrète) liées mathématiquement à partir d'un nombre. Sachant que même avec la clé P (publique) et le message codé on ne peut retrouver la clé S (secrète).
2)B envoie la clé P à A.
3)A chiffre son message (m) avec P : P (m) et l'envoie.

4)B reçoit le message P (m) et le déchiffre avec sa clé privée :
S (P (m))=message.
Si A désire envoyer un message, il procédera de la même façon, il créera un jeu de clés. Au final on aura créer quatre clés.
Ce système permet aussi l'authentification : A chiffre un message avec sa clé privée, B déchiffre ce message avec la clé publique de A. (seul A peut chiffrer avec la clé privée de A. Tout le problème réside à trouver deux fonctions mathématiques (P et S) liées pour que l'une puisse chiffrer et l'autre déchiffrer tout en ne permettant pas que l'on puisse en déduire une à partir de l'autre.
A partir de ces bases, en 1977, D.Rivest, A.Shamir et L.Adleman, ont développé un algorithme répondant à cette problématique. Cet algorithme, le RSA (du nom de ses inventeurs) est toujours utilisé à ce jour.
Principe de base de RSA : A partir du produit de deux grands nombres premiers, p et q, d'une centaine de chiffres chacun, on déduit un nombre entier n : n=pq. La donnée de n est la clé publique (elle suffit pour chiffrer), p et q constituent la clé privée, qu'il faut connaître pour décrypter. Il est très difficile de retrouver les facteurs p et q à partir de n. En pratique, à cause de leur lenteur, les algorithmes à clés publiques sont inutilisables pour des applications nécessitant de nombreux échanges de clés. On utilise alors des algorithmes à clé mixte.
Clé mixte :
Ce principe fait appel aux deux techniques précédentes, à clé symétrique et à clé publique, combinant les avantages des deux tout en évitant leurs inconvénients. Le principe général consiste à effectuer le chiffrement des données avec des clés symétriques, mais en ayant effectué au départ l'envoi de la clé symétrique par un algorithme à clé publique.

9.5.2.2. La signature électronique:

Nous venons de voir les techniques permettant de coder un texte afin de l'envoyer en toute sécurité et le décoder à son arrivée. Reste les problèmes de l'identification de l'expéditeur et l'intégrité des données. La signature électronique permet d'identifier et d'authentifier l'expéditeur des données tout en vérifiant l'intégrité des données, du moins pour la deuxième méthode.
Signature à clés publiques :
Principe de fonctionnement entre un expéditeur A et un destinataire B, il y a deux couples de clés, clé publique/privée A (PA, SA) et B (PB, SB):

- 1.phase d'envoi : A code son message avec sa clé secrète : SA (m), puis avec la clé publique de B : PB (SA (m)) et l'envoie à B.
- 2.phase de réception : B décode avec sa clé privé : SB (PB (SA (m)))=SA (m), seul lui peut faire ce calcul (=sécurité de l'envoi). Puis avec la clé publique de A, il décode le message : PA (SA (m))=m, ce qui certifie A (seul A peut utiliser SA).

Ce fonctionnement est très lent, utilisation de deux paires de clés et il n'y a pas de contrôle d'intégrité des données.
Signature avec hachage :
Le hachage consiste à calculer un résumé très petit du message, ce résumé (appelé digest ou haché) ne doit pas permettre de reconstituer le texte initial s'il est pris tout seul, et il doit être sensible, c'est-à-dire que toute modification du message provoque une modification du résumé. Donc en comparant le résumé et le message, on peut s'assurer de l'intégrité du message. Cette technique couplée à la cryptographie à clé publique permet aussi l'authentification de l'expéditeur.
Exemple :

- 1.phase d'envoi : A calcule le résumé H (m) le code avec sa clé privé SA (H (m)) et code avec la clé publique de B le message: PB (m)), il les envoie à B.
- 2.phase de réception : B décode le message avec sa clé privée : SB (PB (m))=m', il résume ce message H (m'). Il décode le résumé reçu avec la clé publique de A : PA (SA (H (m))), si H (m')= H (m) alors A est bien authentifié et le message est correct.

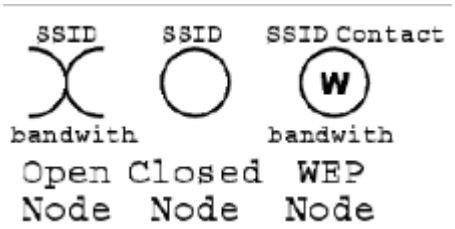
Les principaux algorithmes sont la série MD (Message Digest) avec notamment MD5 qui est très utilisé.

1.1.1. TYPES D'ATTAQUES :

On peut classifier les attaques en deux groupes principaux : les attaques passives et les attaques actives, qui sont bien évidemment plus dangereuses.

9.5.2.3. Attaques passives :

Dans un réseau sans fil l'écoute passive est d'autant plus facile que le média air est difficilement maîtrisable. Bien souvent, la zone de couverture radio d'un point d'accès déborde du domaine privé d'une entreprise ou d'un particulier. L'attaque passive la plus répandue est la recherche de point d'accès. Cette attaque (appelée Wardriving) est devenu le " jeu " favori de nombreux pirates informatique, les points d'accès sont facilement détectables grâce à un scanner (portable équipé d'une carte WIFI et d'un logiciel spécifique de recherche de PA.) Ces cartes wifi sont équipées d'antennes directives (type Yagi) permettant d'écouter le trafic radio à distance hors de la zone de couverture du point d'accès. Il existe deux types de scanners, les passifs (Kismet, Wifiscanner, Prismstumbler…) ne laissant pas de traces (signatures), quasiment indétectables et les actifs (Netstumbler, dstumbler) détectables en cas d'écoute, ils envoient des " probe request ". Seul Netstumbler fonctionne sous Windows, les autres fonctionnent sous Linux.
Les sites détectés sont ensuite indiqués par un marquage extérieur (à la craie) suivant un code (warchalking) :



Une première analyse du trafic permet de trouver le SSID (nom du réseau), l'adresse MAC du point d'accès, le débit, l'utilisation du cryptage WEP et la qualité du signal. Associé à un GPS, ces logiciels permettent de localiser (latitude longitude) ces point d'accès.
A un niveau supérieur des logiciels (type Aisnort ou Wepcrack) permettent, en quelques heures (suivant le trafic), de déchiffrer les clés WEP et ainsi avec des outils d'analyse de réseaux conventionnels la recherche d'informations peut aller plus loin. Le pirate peut passer à une attaque dite active.

9.5.2.4. Attaques actives :

Nous allons revoir, assez succinctement, les différentes attaques connues dans les réseaux filaires et qui touchent, bien évidemment, le monde du wifi.

- DoS (Denial of Service) :

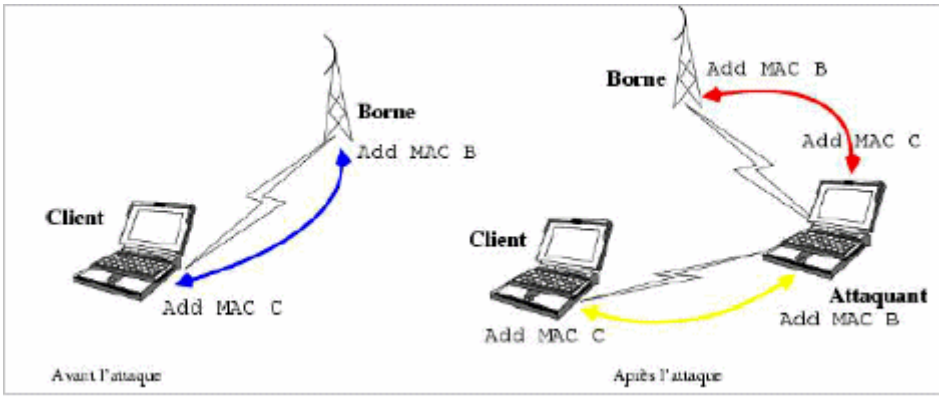
Le déni de service réseau est souvent l'alternative à d'autres formes d'attaques car dans beaucoup de cas il est plus simple à mettre en oeuvre, nécessite moins de connaissances et est moins facilement traçable qu'une attaque directe visant à entrer dans un système pour en prendre le contrôle. Cette attaque a pour but d'empêcher des utilisateurs légitimes d'accéder à des services en saturant de fausses requêtes ces services. Elle se base généralement sur des " bugs " logiciel.
Dans le milieu wifi, cela consiste notamment à bloquer des points d'accès soit en l'inondant de requête de désassociation ou de désauthentification (programme de type Airjack), ou plus simplement en brouillant les signaux hertzien.

- Spoofing (usurpation d'identité) :

Le spoofing IP est une technique permettant à un pirate d'envoyer à une machine des paquets semblant provenir d'une adresse IP autre que celle de la machine du pirate. Le spoofing IP n'est pas pour autant un changement d'adresse IP. Plus exactement il s'agit d'une mascarade (il s'agit du terme technique) de l'adresse IP au niveau des paquets émis, c'est-à-dire que les paquets envoyés sont modifiés afin qu'ils semblent parvenir d'une machine.

- Man in the middle (home au milieu) en milieu Wi-Fi :

Cette attaque consiste, pour un réseau Wi-Fi, a disposer un point d'accès étranger dans à proximité des autres PA légitimes. Les stations désirant se connecter au réseau livreront au PA " félon " leurs informations nécessaires à la connexion. Ces informations pourront être utilisées par une station pirate. Il suffit tout simplement à une station pirate écoutant le trafic, de récupérer l'adresse MAC d'une station légitime et de son PA, et de s'intercaler au milieu.



9.5.2.5. SOLUTIONS INTERNES STANDARDISEES :

Ces solutions sont implantées sur la totalité du matériel standardisé 802.11.

9.5.2.5.1. Accès réseau :

Le premier mécanisme de sécurité de 802.11 est le contrôle d'accès par identifiant du réseau ou SSID (Service Set ID). Toutes les stations et tous les points d'accès appartenant au même réseau possèdent le même SSID (mode infrastructure et Ad-Hoc). Toutes stations voulant se connecter à un réseau 802.11 doit fournir ce SSID au point d'accès. C'est le seul mécanisme de sécurité obligatoire dans Wi-Fi.
Cette protection est très sommaire, car le point d'accès envoie périodiquement en clair cet identifiant dans des trames balises, le réseau est dit " ouvert ". Une simple écoute permet de récupérer le SSID du réseau. Par ailleurs il suffit de spécifier comme SSID le mot " any " dans la configuration de la carte Wi-Fi de la station, pour récupérer tous les SSID des réseaux ouverts. Certain constructeurs offrent la possibilité d'empêcher les broadcasts de SSID du point d'accès, on dit que le réseau est fermé, on ne peut pas fermer des réseaux en mode Ad-Hoc. Par contre on ne peut pas empêcher totalement la diffusion du SSID, car lors de la phase d'authentification entre une station et un point d'accès, il est transmis en clair.
De plus les points d'accès possèdent un SSID par défaut propre à chaque constructeur, si cet SSID n'est pas modifié par l'utilisateur, il est facilement trouvable.
Il en va de même pour le mot de passe nécessaire à la configuration du pont d'accès, celui- ci doit être modifié par l'utilisateur.

9.5.2.5.2. Liste de contrôle d'accès :

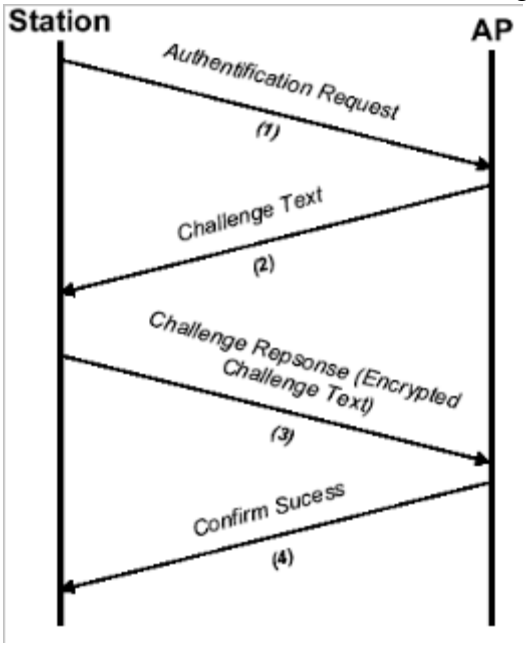
Cette protection consiste à n'autoriser l'accès au réseau qu'à des stations dont l'adresse MAC a été enregistrée dans une liste. Il est très facile pour un pirate de récupérer une adresse autorisée, vu que celles-ci sont transmises en clair, et de la substituer avec la sienne. Donc il s'agit d'une protection très facilement contournable.

9.5.2.5.3. WEP (Wired Equivalent Privacy) :

Fonctionnement
Le standard 802.11 a développé un protocole de sécurisation pour protéger les réseaux sans fil de façon tout aussi efficace que pour les réseaux filaires : le WEP. Ce protocole répond aux trois principes fondamentaux de sécurité : authentification, confidentialité des données, et intégrité des données.
Ces principes se basent sur un système à clé symétrique, la même clé étant utilisée pour chiffrer et déchiffrer les données. Cette clé est partagée par tous les clients du réseau et par le point d'accès. Il y a deux longueurs de clé possible, 64 et 128 bits (sachant que 24 bits servent pour l'initialisation de la clé).
·Authentification : le mécanisme d'authentification utilise la clé partagée pour l'envoi des données chiffrées. Il existe deux mécanismes d'authentification :

- Open System Authentication : mécanisme par défaut, il n'y a pas d'authentification véritable, toute station désirant se connecter, est automatiquement authentifiée.
- Shared Key Authentication : ce mécanisme se déroule en quatre étapes :
  - 1.la station envoie une requête d'authentification au point d'accès.
  - 2. le PA envoie un texte en clair 128 bits généré par l'algorithme WEP.
  - 3. la station chiffre ce texte avec la clé partagée et l'envoie dans une trame d'authentification.

- 4. le PA déchiffre le texte reçu avec la même clé partagée et le compare avec le texte précédent, s'il y a égalité il confirme à la station son authentification et la station peut alors s'associer. Sinon le PA envoie une trame d'authentification négative.

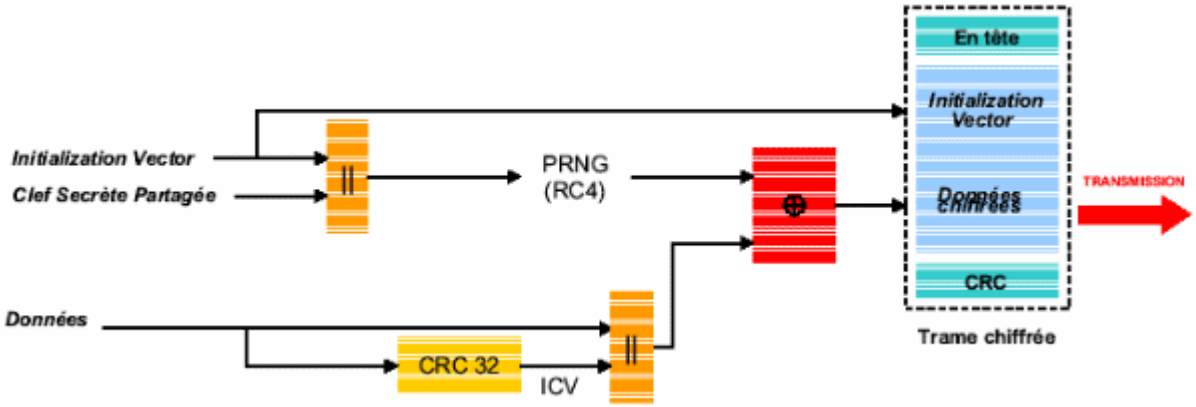


·Chiffrement et contrôle d'intégrité : Le mécanisme de chiffrement et de contrôle d'intégrité du WEP se base sur l'algorithme RC4, développé par Ron Rivest en 1987 pour RSA Security. C'est un algorithme à clé symétrique secrète. L'authentification permet de s'assurer que la station possède bien la clé. Le chiffrement et le contrôle d'intégrité se déroulent en plusieurs étapes :

- 1.Elaboration du Key Scheduling Algorithme : On concatène (ajoute) la clé partagée (40 ou 104 bits) et un vecteur d'initialisation de 24 bits (IV : Initialisation Vector qui change à chaque trame envoyée), formant ainsi la graine (seed) de RC4 appelé aussi Key Scheduling Algorithme (64 ou 128 bits). â [Key¦IV] *
- En parallèle on effectue, avec un CRC 32, un calcul d'intégrité (non chiffré) ou ICV (Integrity Check Value) sur les données. Les données sont, ensuite, concaténées avec cet ICV. â [Data¦ICV] *
- 2.Cette graine est placée dans un générateur de nombre pseudo aléatoire (PRNG : Pseudo Random Number Generator) qui crée une séquence pseudo aléatoire. â [PRNG (Key¦IV)] *
- 3.On applique un XOR (opération logique de OU exclusif) bit à bit entre cette séquence et les données concaténées avec l'ICV, formant ainsi les données cryptées. â [(Data¦ICV)Å(PRNG (Key¦IV))] *
- 4.Les données chiffrées sont transmises et l'IV est rajouté à la trame.
  Remarque : le chiffrement n'est appliqué que sur les données de la trame MAC, l'en-tête, l'IV et le CRC sont transmis en clair.

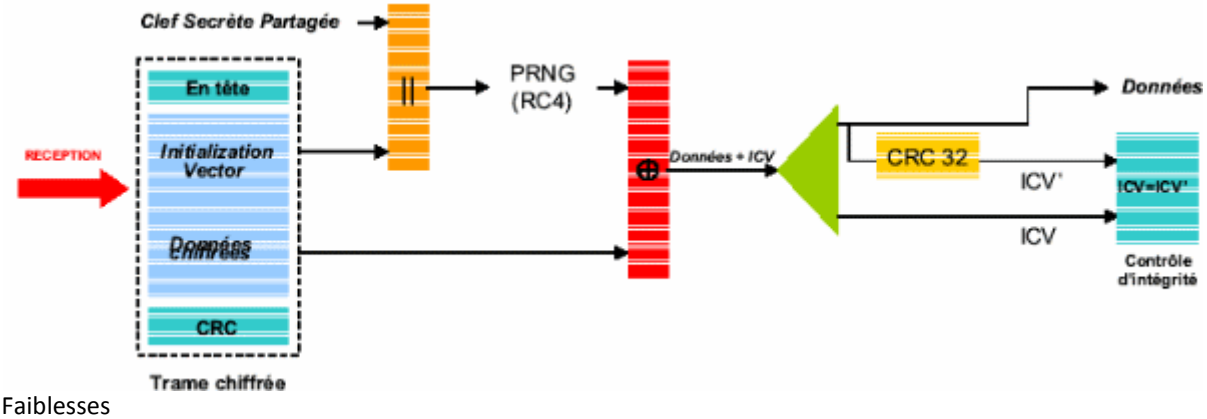
* :¦= concaténation ; Å = " ou " exclusif

·Déchiffrement et contrôle d'intégrité : Le déchiffrement et le contrôle d'intégrité se déroulent en plusieurs



étapes comme précédemment, mais en sens inverse :

- La clé partagée est concaténée avec l'IV de la trame reçue, puis l'ensemble est introduit dans le PRNG pour donner la bonne séquence pseudo aléatoire qui a été utilisé pour le chiffrement.
- 2. On effectue un XOR entre cette séquence aléatoire et les données chiffrées reçues. On obtient les données et l'ICV en clair.
- 3. On effectue un contrôle (ICV') sur ces données en clair que l'on compare avec l'ICV reçu. Si ICV'=ICV on peut être sûr des données.



·Faiblesses

Il existe des faiblesses propres à l'algorithme RC4 utilisé mais aussi à la conception de WEP. La principale vient de la clé qui est fabriquée par la concaténation d'une clé unique, partagée par tous les membres du réseau et d'une longueur maximale de 104 bits, et d'un vecteur d'initialisation. Cette clé est trop courte et l'IV est transmis en clair, on peut donc facilement au bout d'un certain temps d'écoute déduire la clé, en sachant que généralement le vecteur d'initialisation démarre à 0 en début de transmission. Tout ceci se faisant avec l'aide de logiciel spécifique de type Airsnort ou Wepcrack. D'autre part le CRC utilisé est trop faible, cela conduit à la possibilité par des pirates de modifier des paquets ou d'injecter de faux paquets dont le CRC a pu être modifié. Une autre faille provient de la séquence d'authentification où un texte en clair est envoyé par l'AP et sa version codée renvoyée par la station. Une simple écoute permet d'obtenir ces deux éléments ce qui permet de calculer beaucoup plus facilement la clé.

Remarque : Tout algorithme de sécurité nécessite de la part du processeur plus de calcul et ceci entraîne une baisse des performances notamment sur le débit. Cette baisse est très variable suivant les cartes, le fait d'activer le WEP peut faire chuter de 5 à 50% le rendement du processeur de la carte Wi-fi.

9.5.2.6. SOLUTIONS INTERNES TEMPORAIRES :

Ces solutions sont implantées aujourd'hui sur la majorité du matériel ou en cours d'implantation au travers de patch software sur une partie du matériel plus ancien.

- WPA (Wi-Fi Protected Access)

Face à la faiblesse du WEP, et en attendant un standard propre à la sécurité des réseaux sans fil 802.11 (norme 802.11i en cours d'élaboration), le groupe de travail IEEE802.11i a développé une solution temporaire : le WPA. Le WPA a le double avantage de pouvoir être implanté sur le matériel déjà existant (remise à jour du firmware) et d'être compatible avec la future norme de sécurité 802.11i. Le WPA est composé de deux éléments :

- TKIP (Temporal Key Integrity Protocol)

Protocole permettant le cryptage et le contrôle d'intégrité des données.

Ce protocole utilise toujours RC4 (d'où sa compatibilité avec le WEP) comme algorithme de cryptage avec une clé de 128 bits, par contre l'IV (vecteur d'initialisation) passe à 48 bits. De plus il y a une clé par station (et non une pour tout le réseau avec WEP), cette clé est générée et changée automatiquement de façon périodique. Le contrôle d'intégrité des données s'effectue par un code de hachage de 8 octets appelé MIC (Message Integrity Code) ou Michael. Ce code porte aussi les adresses MAC, ce qui évite de modifier ou forger des trames. De plus il utilise un numéro de séquence sur les paquets, permettant un contrôle de bon séquencement.

- 802.1x :

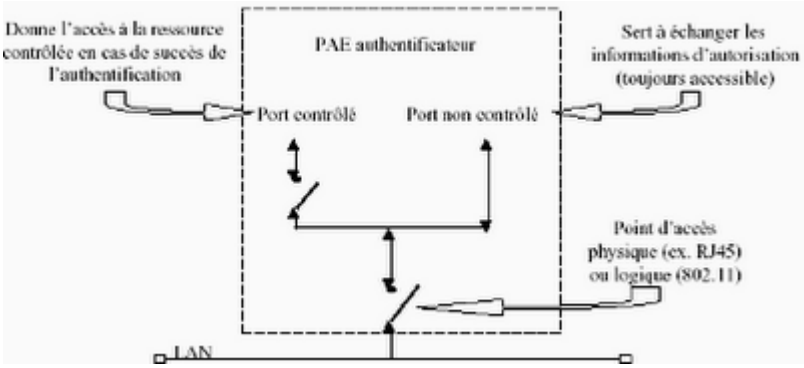
Protocole permettant l'authentification.

Ce protocole, datant de 2001, est l'évolution de différents protocoles (PPP, RADIUS, EAP) développés pour l'authentification. Ce protocole vise à standardiser un mécanisme de relais d'authentification au niveau 2 que ce soit un réseau filaire ou sans fil, et à contrôler l'accès aux ressources si l'accès physique n'est pas contrôlable

(ce qui est le cas dans un environnement radio). Nous allons voir son application dans le milieu des RLAN.
Les éléments :
Le protocole fonctionne à partir de trois éléments :

- Le client (station) ou système à authentifier.
- -Le contrôleur (point d'accès) ou système authentificateur.
- -Le serveur d'authentification (serveur placé sur le LAN).

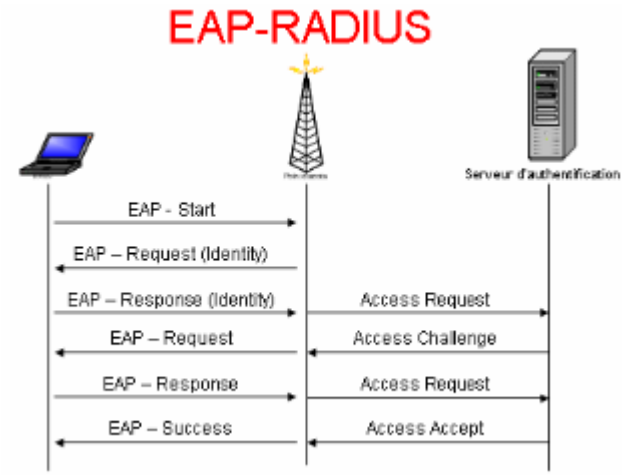
802.1x est aussi appelé Port-based Network Access Control, c'est-à-dire qu'il introduit une notion de port contrôlé par l'authentification. Une station ne pourra accéder aux ressources d'un LAN que si elle a été auparavant authentifiée.
Fonctionnement :
Concrètement la station va se connecter au point d'accès par un PAE (Port Access Entity), ce PAE est divisé en deux ports, un port contrôlé (connexion ouverte ou fermée) donnant accès à la ressource en cas de succès de l'authentification, et un port non contrôlé (connexion toujours ouverte) servant à l'authentification où tout autre trafic est rejeté.



Le port contrôlé peut être ouvert ou fermé suivant le contrôle qui a été défini au moyen d'une variable (AuthControlledPortControl). Cette variable peut prendre trois états :

- ForceUnauthorized : l'accès au port contrôlé est interdit (connexion toujours ouverte).
- ForceAuthorized : l'accès au port contrôlé est autorisé (connexion toujours fermée).
- Auto (par défaut) : l'accès dépend du résultat de l'authentification.
- Authentification par RADIUS :

On utilise le protocole EAP pour véhiculer l'authentification lors d'une session, EAPOL (Extensive Authentication Protocol Over Lan) entre la station et le point d'accès et EAP entre le PA et le serveur (on utilise surtout un serveur RADIUS : Remote Authentication Dial In User Server). Ce protocole peut encapsuler tous les protocoles d'authentification.



Généralement la station et le serveur partage un secret (clé, certificat), et dés que le serveur reçoit une requête du point d'accès pour une station, il renvoie un challenge à la station. Ce challenge ne peut être résolu que par ce secret partagé et permettre ainsi l'authentification. Différents type de protocoles sont possibles :
·Types d'authentifications :

- authentification par mot de passe : EAP-MD5, il est de moins en moins utilisé ; LEAP (Light EAP) protocole propriétaire Cisco.
- authentification par carte à puce : EAP-SIM (Subsciber Identity Module), utilisé pour les points d'accès public (hot spot), utilise la carte à puce SIM du GSM, permet la mise en place de facturation ; EAP-AKA (Authentification and Key Agreement), utilise le système d'authentification de la carte SIM de l'UMTS, il est compatible avec le GSM.
- authentification par certificat : EAP-TLS (Transport Layer Security), basé sur les mécanismes SSL (Secure Socket Layer) est très utilisé, il utilise une infrastructure à clé publique PKI, il génère et distribue des clés WEP dynamique (par utilisateur, par session et par paquet). Nécessite un certificat pour chaque client.

Pour palier à certaines faiblesses du protocole EAP (défaut de protection de l'identité de l'utilisateur, problème lors de reconnexion rapide…), le protocole PEAP (Protected EAP) a été développé. Ce protocole utilise MS-CHAP v2 pour l'authentification.

Infrastructure	**Radius** AAA Kerberos LDAP
Méthodes d'authentification	**LEAP TLS PEAP** TTLS MD5 GSM-SIM
Protocole d'authentification	**EAP**
Média	**802.1x** 802.3 802.11 802.16 PPP

Remarque : WPA fonctionne sur Windows 2000 et XP (Service Pack 1), avec 802.11a 802.11b et 802.11g.

9.5.2.7. SOLUTIONS INTERNES FUTURES :

9.5.2.7.1. 802.11i (RSN: Robust Security Network):

Comme je l'ai expliqué précédemment, le WPA est temporaire et la norme définitive 802.11i devrait être ratifié en 2004. Cette norme doit palier les manques de WPA et apporter des solutions sur différents points : un SSID sécurisé, une déconnexion rapide et sécurisée, dé authentification et dé association sécurisées, mise en place de AES en remplacement de RC4. Mise en place d'une authentification mutuelle station et point d'accès.

9.5.2.7.2. AES-CCMP (Advanced Encryption Standard-Counter mode with CBC Mac Protocol):

protocole remplaçant TKIP et utilise AES à la place de RC4. AES est un algorithme de cryptage très puissant à clé symétriques mais nécessite une grosse puissance de calcul et ne peut être utilisable par les cartes actuelles.

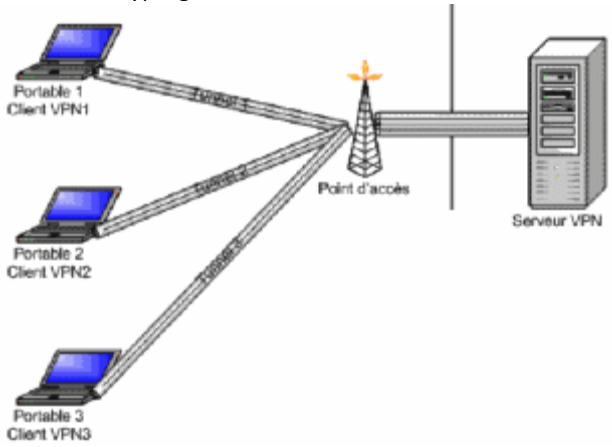
9.5.2.8. SOLUTIONS EXTERNES

9.5.2.8.1. VPN (Virtual Private Network)

Après avoir vu la sécurisation au niveau des données, nous allons voir les moyens existant pour sécuriser un réseau et en particulier à travers le concept de réseau privé virtuel.

Le rôle initial d'un VPN est de permettre à un utilisateur éloigné de son entreprise de se connecter en toute sécurité au LAN de celle-ci en passant par des réseaux qui ne sont pas sécurisés. De nos jours les VPN sont très utilisés dans les LANs d'entreprise pour assurer des échanges sécurisés et une qualité de service. Il répondent

aux trois besoins fondamentaux : Cryptage des données, authentification des hôtes, contrôle d'intégrité.



PPTP : c'est un protocole de niveau 2 développé par Microsoft, permettant à des connexions PPP (Point to Point Protocol) d'être sécurisées (codage, authentification) tout en étant convoyées dans un réseau IP à travers un tunnel virtuel. Il utilise Le protocole d'authentification dans Microsoft PPTP est le protocole d'épreuve/réponse de Microsoft (MS-CHAP : Microsoft Challenge Handshake Authentication Protocol) le protocole de chiffrement est le chiffrement MPPE (Microsoft Point-to-Point Encryption). Celui-ci utilise un algorithme de chiffrement RC4 en 40 ou 128 bits. La version actuelle est MS-CHAPv2. Microsoft a amélioré PPTP afin de corriger les failles majeures de sécurité.
L2TP : Protocole de niveau 2 qui encapsule des trames PPP pour les envoyer des réseaux IP, mais aussi de type WAN (X25, Frame relay, ATM) L2TP a été conçu pour transporter des sessions PPP au travers d'un réseau, et de terminer physiquement les sessions PPP en un point de concentration déterminé dans le réseau. Avec L2TP, on identifie les deux parties essentielles du tunnel comme suit :
LAC (L2TP Access Concentrator) : il s'agit de l'équipement faisant l'adaptation réseau d'accès (type RTC, numéris, ADSL, etc.) au réseau IP. Le rôle du concentrateur d'accès LAC se limite à fournir un support physique qui sera utilisé par L2TP pour transférer le trafic vers un ou plusieurs serveurs réseau L2TP (LNS). Il assure le fractionnement en canaux pour tout protocole basé sur PPP. Le concentrateur d'accès LAC joue le rôle de serveur d'accès : il est à l'origine du tunnel et est responsable de l'identification du VPN.
LNS (L2TP Network Server) : Il s'agit de l'équipement sur le réseau terminant les sessions PPP et aggrégant l'ensemble des sessions. Les serveurs LNS sont les émetteurs des appels sortants et les destinataires des appels entrants. Ils sont responsables de l'authentification du tunnel.
La création d'un tunnel PPP avec L2TP se déroule en deux phases :

- établissement d'une connexion de contrôle entre le LAC et le LNS pour ouvrir un tunnel L2TP, permettant une identification du LAC et du LNS.
- établissement d'une session L2TP suite à la réception d'un appel rentrant ou sortant du LAC. De multiples sessions peuvent utiliser le même tunnel et de multiples tunnels peuvent être créés entre un couple LAC, LNS.

La session L2TP est maintenu par des trames « Hello »d'entretien (keepalive).
IPsec :
IPsec permet de sécuriser les échanges au niveau de la couche réseau, en fournissant de la confidentialité (cryptage), une authentification (source et destinataire), de l'intégrité des données. Il fonctionne suivant deux mécanismes :

- AH (Authentication Header) : ce protocole permet l'authentification de la source et l'intégrité des données, on ajoute un bloc de données (appelé ICV :integrity check value obtenu par un algorithme de hachage) après l'entête IP.
- -ESP (Encapsulating Security Payload) : ce protocole permet en plus de l'authentification et de l'intégrité, la confidentialité grâce au chiffrement. Il chiffre les données originales qui sont ensuite encapsulées entre un entête et un enqueue.

IPsec fonctionne suivant deux modes :

- le mode tunnel : utilisé pour les tunnels entre des équipements réseaux, permet la protection de tous les champs des datagrammes IP.
- le mode transport : ne protége que les données du datagrammme IP et pas les entêtes. Il est utilisé pour les connexions entre les équipements terminaux.

9.6. STANDARDS CONCURRENTS

9.6.1. HOME RF

Generalités :
Lancé en Mars 1998 le Home Radio Frequency Working Group (HomeRF WG) composé de Compaq, HP, IBM, Intel et Microsoft, a développé un protocole SWAP (Shared Wireless Access Protocol) permettant le transport de la voix et des données grâce à une technique sans fil à usage domestique, pour un débit de 1,6 Mbits/s à 20 Mbits/s. Un réseau SWAP fonctionne avec trois types d'unités, un point de contrôle, une unité pour la voix (mode isochrone), une unité pour les données (mode asynchrone). Le protocole SWAP travaille aussi bien en mode peer to peer pour les échanges de données qu'en mode client serveur pour le transfert de la voix.
Les réseaux Home RF sont sécurisés par un algorithme de sécurité à clés de 58 bits.
Couche 2 :
La couche MAC utilise un protocole TDMA (Time Division Multiple Access), protocole à multiplexage temporel, pour le transport de la voix et un protocole CSMA /CA (Carrier Sense Multiple Acces/ Collision Avoidance) pour les données.
Couche 1 :
Home RF fonctionne dans la bande des 2,4 GHz en utilisant une technologie à saut de fréquences (FHSS Frequency Hope Spread Spectrum, à 50 sauts/s).
Conclusion :
Cette norme ne s'est jamais implantée en Europe, et l'apparition de 802.11b n'a fait qu'accentuer son déclin.

9.6.2. HIPERLAN

- HIPERLAN 1

L'ETSI a développé HiperLan 1 (1996) et HiperLan 2 (1999), pour concurrencer la norme américaine 802.11. Cette norme fonctionne dans la bande de fréquence des 5,15-5,30 GHz et possède un débit de 23,5 Mbits/s pour une portée moyenne d'environ 50 mètres pour les équipements les plus puissants. L'architecture d' HiperLan 1 est de type décentralisé, il n'y a pas de notion de point d'accès, par contre un nœud peut fonctionner en pont. Caractéristiques principales d'HiperLan1 :

- Un système d'accès multiple doté de priorités appelé EY-NPMA (Elimination Yield-Non Preemptive Multiple Access). Mélange de détection de porteuse de type CSMA et de signalement actif de priorité permettant de gérer cinq niveaux de priorité. Il 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.
- Une technique de relayage de trames permettant d'étendre un réseau local dont l'extension dépasse la portée radio. Pour cela la norme distingue deux types de nœud ; des nœuds relais (forwaders) permettant de recevoir des paquets (qui ne leurs sont pas destinés) pour les relayer vers une destination finale ; et des nœuds simples (non forwaders). Pour cela la trame possède une paire d'adresse MAC traditionnelles mais aussi une autre paire, désignant les nœuds intermédiaires et faisant partie de l'encapsulation CAC (Channel Access Control).
- Cette technique se base sur un algorithme permettant de construire automatiquement la topologie du réseau. L'architecture de ce réseau se développe à travers des trames de type " Hello ", permettant à un nœud de connaître son voisinage proche, et des trames de contrôle de topologie, sorte de table de routage, diffusées sur tout le réseau.

- HIPERLAN 2

Fondé en 1999 par différentes sociétés (Bosch, Dell, Ericsson…) l'H2GF (Hiperlan 2 Global Forum) soutient le projet HiperLan 2.
Cette norme est en concurrence directe avec 802.11a, elle fonctionne sur la bande des 5GHz en modulation OFDM (voir norme 802.11) avec un débit de 54Mbits/s. Son architecture est de type centralisé avec un mode appelé réseau d'accès ressemblant au mode infrastructure Wi-Fi, où chaque terminal se rattache à un point d'accès. Et une architecture de type Ad-Hoc mais où une station appelée Central Controler (CC) devient le point d'accès.
Par-dessus cette architecture Hiperlan2 fonctionne suivant deux modes :

- mode centralisé : tous les paquets passent par le point d'accès.
- mode direct : deux terminaux peuvent communiquer directement sans passer par un PA ou un CC.

Fonctionnalités :

- Haut débit : la couche physique peut transmettre et recevoir des données à 54 Mbits/s grâce à la modulation OFMD.
- Mode orienté connexion : avant chaque envoi, une connexion est établie entre les stations 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 toutes les stations en même temps.
- QoS : du fait que les communications sont en mode connectée, 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 terminal 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.

L'architecture générale est composée de trois couches :

- CL : Convergence Layer (couche de convergence). Elle permet d'interfacer différents types de réseaux classiques (à cellules types ATM ; à paquets type Ethernet, TCP/IP ; ou UMTS) en adaptant des services demandés par les couches hautes aux services proposés par la couche DLC.
- DLC : Data Link Control (couche contrôle liaison de données): une première sous-couche est divisée en deux parties.
- RLC (Radio Link Control) : protocole gérant tous les aspects de contrôle des connexions aux travers de trois sous groupes. ACF gère les associations et désassociations ainsi que le chiffrement ; RRC permet la sélection automatique des fréquences et de la meilleure puissance et gère le handover ; DCC s'occupe du contrôle des connexions.
- EC (contrôle d'erreurs) : permet de contrôler les données et ainsi d'augmenter la fiabilité de la connexion.

Conclusion :

Malgré une conception élaborée et des fonctionnalités supérieures au Wi-fi les normes HiperLan ne sont pas commercialisées. La norme HiperLan 1 ne dépassera pas le stade de prototype. Quant à HiperLan 2, sa conception est en concurrence directe avec 802.11a et a peu de chance de se développer un jour.

9.6.3. 802.15.3

Ce nouveau standard de l'IEEE publié en Août 2003 par le groupe de travail 802.15, a été conçu pour le transfert de fichier audio ou vidéo nécessitant des hauts débits. Ce standard définit un débit de 55Mbits/s sur une portée de 100 mètres, diffusé sur la fréquence des 2,4GHz et garantit sans interférences avec les normes de types 802.11x, 802.15x et Bluetooth.

De plus il inclut le protocole TDMA permettant de gérer des connexions simultanées et l'algorithme de cryptage AES pour un niveau de sécurité élevé.

9.6.4. 802.15.3a (UWB: Ultra Wide Band)

Dernière norme en cours de préparation tirée d'une technologie militaire utilisée dans le domaine des radars GPR (Ground Penetring Radar) capables de détecter des éléments au travers de toutes sortes de matières (eau, terre, béton...). Contrairement à la technologie sans fil classique qui envoie un signal sur une largeur de bande étroite, l'UWB envoie des millions de signaux courts de faible puissance sur un spectre de fréquences ultralarge. Les principaux avantages sont : débit très importants (110 à 480 Mbits/s), une faible consommation, pas de contrainte de topologie (les ondes traversent les murs), difficultés d'interception des ondes (temps de transmission court et changement de fréquences).

Par contre, comme UWB utilise un spectre très large de fréquences, les organismes de réglementation craignent une perturbation des canaux de communication existants. Aux Etats- Unis, après trois ans de test, la FCC a donné son accord pour la vente de systèmes UWB pour certaines applications dont la transmission sans fil à l'intérieur des bâtiments.
De nombreux constructeurs voient dans cette technologie, le remplaçant à toutes les autres.