

# Table des matières

<b>1. INTRODUCTION</b> .....	2
<b>2. HISTORIQUE</b> .....	2
<b>3. DÉFINITION</b> .....	4
<b>4. A QUOI SERT LE PÉRIPHÉRIQUE</b> .....	4
<b>5. PRINCIPE PHYSIQUE</b> .....	4
A) L'ADRESSE MAC .....	4
B) L'IRQ .....	5
C) DMA .....	6
D) L'ADRESSE DE BASE E/S .....	7
E) LE TRANSCIVER .....	8
F) LE PLUG-AND-PLAY .....	8
G) TRANSMISSION DE DONNÉES ENTRE 2 CARTES RÉSEAUX .....	9
<b>6. CARACTÉRISTIQUES D'UN RÉSEAU</b> .....	11
<b>7. STRUCTURE HARDWARE</b> .....	12
➤ L'INTERFACE : LES BUS .....	12
➤ LES CONNECTEURS .....	13
➤ LE CÂBLAGE .....	14
<b>8. LE WIFI</b> .....	18
<b>9. LES 2 GRANDS RÉSEAUX</b> .....	24
L'ARPANET .....	24
L'INTERNET .....	25
<b>10. TOPOLOGIES DES RÉSEAUX</b> .....	27
<b>11. INSTALLATION D'UNE CARTE RÉSEAU</b> .....	29
<b>12. L'AVENIR DE LA CARTE RÉSEAU - CONCLUSION</b> .....	34
• EXEMPLES DE CARTES RÉSEAUX ACTUELLEMENT SUR LE MARCHÉ .....	34
<b>RÉFÉRENCES</b> .....	35

# Périphérique : La carte réseau

## **1. Introduction**

Dans le cadre du cours de réseau, il nous est demandé de présenter un périphérique au choix. Notre choix s'est porté sur la carte réseau. Ce périphérique permet une fonction très importante dans l'informatique : Echanger ou Communiquer. Du plus petit partage entre deux systèmes jusqu'à la mise en commun à distance par la toile, ce périphérique a su s'imposer comme utile et se voit évoluer maintenant sous différentes formes. Nous allons présenter dans ce travail cette interface réseau ainsi que ses évolutions actuelles en passant le plus brièvement par ce qui nous a été présenté au cours de réseau pour ne pas répéter des notions acquises.

## **2. Historique**

L'ordinateur est un outil très pratique mais, une fois en réseau, l'étendue de ses possibilités devient pratiquement infinie ! Voici l'histoire des moyens de communication et des réseaux informatiques qui ont permis l'apparition d'Internet.

*1955* : Premier réseau informatique à but commercial : SABRE (Semi Automated Business Related Environment) réalisé par IBM.

*1958* : La BELL crée le premier **Modem** permettant de transmettre des données binaires sur une simple ligne téléphonique.

*Juillet 1961* : Leonard Kleinrock du MIT publie une première théorie sur **l'utilisation de la commutation de paquets** pour transférer des données.

*1965* : Lawrence G. Roberts va, avec Thomas Merrill, connecter l'ordinateur TX-2 au Massachussets avec l'ordinateur Q-32 en Californie par une liaison téléphonique. Cette expérience va prouver la faisabilité et l'utilité d'un réseau d'ordinateurs.

*Septembre 1969* : BBN installe le premier équipement réseau IMP (basé sur un mini-ordinateur Honeywell 516 avec 12 Ko de Ram, voir photo ci-contre) à l'UCLA et le premier ordinateur (XDS SIGMA 7) y est connecté. Un ordinateur (XDS 940) de l'équipe de Douglas C. Engelbart de la Stanford Research Institute est alors relié via une **liaison à 50 kbits/s**. Les premières données sont échangées entre ces machines.

*1969* : Création de la norme de connexion série **RS232**.

*Décembre 1970* : Le Network Working Group termine le protocole de communication entre ordinateurs pour le réseau ARPANET appelé **Network Control Protocol** ou **NCP**.



*Mars 1972* : **Ray Tomlinson** de **BBN** réalise la première application réseau majeure pour **ARPANET** : un logiciel basique de **courrier électronique** répondant au besoin de communication des développeurs du réseau.

*1972 - 1973* : Bob Kahn et Vinton Cerf travaillent en coopération sur un nouveau protocole palliant aux failles du protocole NCP. C'est ainsi que fut créé **TCP/IP** (Transmission Protocol, Internet Protocol).

*1973* : **Bob Metcalfe** met au point l'interface réseau **Ethernet** chez **Xerox** en s'inspirant des principes du réseau informatique radio de l'université de Hawaï : Alohanet.

*1976* : Les laboratoires **Bell** d'**AT&T** développent **UUCP** (Unix to Unix Copy Program). Il s'agit du premier protocole d'échanges de données largement disponible et qui sera énormément utilisé avant l'avènement de **TCP/IP** et d'**Internet**.

*1978* : Le CCITT définit le modèle **OSI** en 7 couches pour amener la standardisation au sein de la jungle des protocoles de communication de tous les constructeurs informatiques.

*1979* : Hayes sort un **modem** 110/300 bauds pour l'Apple II. Il est vendu 380 \$.

*1982* : Le réseau **EUnet** (European Unix network) est mis en place pour interconnecter les machines européennes et permettre la circulation de l'email et des news USENET. Les premiers pays raccordés sont la Hollande, le Danemark, la Suède et l'Angleterre.



*1984* : **Sandy Lerner** et **Len Bosack** fondent la société **Cisco Systems** dans le salon de leur maison (Cf. photo !) pour fabriquer et vendre les premiers **Routeurs** permettant d'interconnecter divers réseaux entre eux pour former un réseau global.

Ils viennent tous deux de l'Université de Stanford où ils ont mis au point le réseau global du campus.

Le nom de la société vient de San Francisco où ils habitaient et le logo de la société est une représentation du Golden Gate bridge.

*1984* : Mise en place du **DNS** (Domain Name Server) sur Internet.

*1985* : La **NSF** (National Science Foundation) forme le réseau **NSFNET** reliant 5 sites équipés de super ordinateurs avec des liaisons à 56 kbits/s : L'université de Princeton, Pittsburgh, l'université de Californie à San Diego, l'université de l'Illinois à Urbana-Champaign et l'université de Cornell.

*1990* : ARPANET cède définitivement la place à Internet

*1991* : Plug-and-play par dévoilée par Microsoft et Intel

*1998* : La norme 802.11 est finalisée.

*1999* : 802.11b prend le nom de wifi.

*2002* : 58 départements Français sont autorisés à utiliser la fréquence 2.4Ghz

*2003* : Autorisation étendue à toute la France.

### **3. Définition**

→ Carte réseau

Les cartes réseau (appelées Network Adapter Card en anglais) constituent l'interface entre l'ordinateur et le câble du réseau.

Une carte réseau est une carte d'extension que l'on installe dans un ordinateur pour permettre à ce dernier de communiquer avec d'autres ordinateurs en réseau .

La plupart des cartes réseau sont conçues pour un type de réseau (Ethernet, Token Ring, X.25, etc.), un jeu de protocoles (pile TCP/IP, IPX, etc.) et un support physique donné (paire de fils de cuivre, câble coaxial de différents diamètres, fibre optique, etc.), mais certaines cartes sont multiréseaux.

Certains ordinateurs sont livrés avec un contrôleur de réseau déjà présent sur leur carte mère et n'ont donc pas besoin de carte réseau supplémentaire. Les cartes réseau disposent de paramètres qu'il est possible de configurer. Parmi eux figurent l'interruption matérielle (IRQ), l'adresse de base du port E/S et l'adresse de base de la mémoire (DMA).

### **4. A quoi sert le périphérique**

La fonction d'une carte réseau est de préparer, d'envoyer et de contrôler les données sur le réseau. Pour préparer les données à envoyer, la carte réseau utilise un transceiver (Interface permettant le raccordement de deux types de câble : AUI/FO, AUI/BNC...) qui transforme les données parallèles en données séries. Une carte réseau sert d'interface physique entre l'ordinateur et le câble. Elle prépare pour le câble réseau les données émises par l'ordinateur, les transfère vers un autre ordinateur et contrôle le flux de données entre l'ordinateur et le câble. Elle traduit aussi les données venant du câble et les traduit en octets afin que l'Unité Centrale de l'ordinateur les comprenne. Ainsi une carte réseau est une carte d'extension s'insérant dans un connecteur d'extensions (slot).

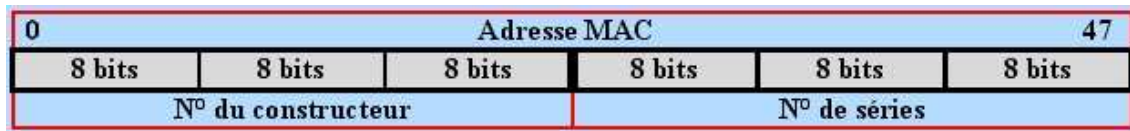
### **5. Principe physique**

Chaque carte dispose d'une adresse unique, appelée adresse MAC, affectée par le constructeur de la carte, ce qui lui permet d'être identifiée de façon unique dans le monde parmi toutes les autres cartes réseau. Pour garantir la compatibilité entre l'ordinateur et le réseau, la carte doit être adaptée à l'architecture du bus de données de l'ordinateur et avoir le type de connecteur approprié au câblage. Chaque carte est conçue pour s'adapter à un certain type de câble. Certaines cartes comprennent plusieurs connecteurs d'interfaces (à paramétrer soit avec les cavaliers, soit avec les DIP, soit de façon logicielle). Les connecteurs les plus répandus sont les connecteurs RJ-45.

NB : Certaines topologies réseau propriétaires utilisant la paire torsadée ont recours au connecteur RJ-11. Ces topologies sont parfois appelées « *pré-10BaseT* » (voir plus loin dans le travail).

#### **a) L'adresse MAC**

L'adresse MAC (Medium Access Control) est présente sur toutes les cartes réseaux. Une adresse MAC (ou adresse physique) est structurée sur 6 octets qui représente 48 bits, les trois premiers octets de 8 bits représente le numéro du constructeur, tandis que les trois octets suivants représentent le numéro de série unique pour chaque carte vendue. Ce numéro est capital car c'est lui qui sert de référence dans un réseau pour déterminer la machine sur laquelle elle se trouve.



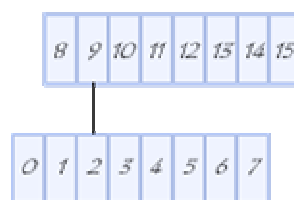
Cette adresse sert d'identification de l'interface sur un réseau. La norme IEEE définit le format et l'assignation d'adresses MAC car chaque adresse doit être en tout état de cause être unique dans un réseau. C'est à dire qu'il n'existe pas deux cartes réseaux avec la même adresse physique. La sous-couche MAC est implémentée au niveau 2 du modèle OSI à l'intérieur de la couche liaison. Vous ne pouvez voir ce numéro lorsque vous regardez une carte réseau, en fait elle est gravée dans une ROM sur la carte réseau. Les adresses MAC sont utilisées et maniées par les commutateurs Ethernet ou bien le protocole ARP. Plus généralement on admettra, que toutes trames traversant la couche 2 du modèle OSI doivent posséder une adresse MAC source et une adresse destinataire.

### b) L'IRQ

Puisque le processeur ne peut pas traiter plusieurs informations simultanément (il traite une information à la fois, le multitâche consiste à alterner des morceaux d'instructions de plusieurs tâches différentes), un programme en cours d'exécution peut grâce à une interruption être momentanément suspendu, le temps que s'exécute une routine d'interruption. Le programme interrompu peut ensuite reprendre son exécution. Il existe 256 adresses d'interruption différentes. Une interruption devient une interruption matérielle lorsqu'elle est demandée par un composant matériel de l'ordinateur. En effet, il existe dans l'ordinateur de nombreux périphériques. Ceux-ci ont généralement besoin d'utiliser les ressources du système, ne serait-ce que pour communiquer avec lui...

Ainsi, lorsque ceux-ci ont besoin d'une ressource, ils envoient parfois au système une demande d'interruption pour que ce dernier leur prête son attention. Ainsi, les périphériques ont un numéro d'interruption, que l'on appelle IRQ (*Interruption request*, ce qui signifie «*requête d'interruption*»). A titre d'image, chaque périphérique tire une «ficelle» reliée à une cloche pour signaler à l'ordinateur qu'il veut qu'il prête attention à lui.

Cette "ficelle" est en fait une ligne physique qui relie le slot à la carte mère. Pour un emplacement ISA 8 bits par exemple, il y a 8 lignes IRQ (Interruption Request Line) qui relient le slot ISA 8 bits à la carte mère, c'est-à-dire IRQ0 à IRQ7. Ces IRQ sont contrôlés par un «contrôleur d'interruption» qui permet de "donner la parole" à l'IRQ ayant la plus grande priorité. Pour les slots 16 bits, les IRQ 8 à 15 ont été ajoutés, il a donc fallu ajouter un second contrôleur d'interruption, la liaison entre les deux groupes d'interruption se fait par l'intermédiaire de l'IRQ 2 reliée à l'IRQ 9 (et appelée «cascade»). La cascade vient donc en quelque sorte "insérer" les IRQ 8 à 15 entre les IRQ 1 et 3 :



La priorité étant donnée par ordre d'IRQ croissant, et les IRQ 8 à 15 étant insérées entre les IRQ 1 et 3, l'ordre de priorité est donc le suivant :

**0 > 1 > 8 > 9 > 10 > 11 > 12 > 13 > 14 > 15 > 3 > 4 > 5 > 6 > 7**

### c) DMA

Des périphériques ont régulièrement besoin d'"emprunter de la mémoire" au système afin de s'en servir comme zone de tampon (en anglais *buffer*), c'est-à-dire une zone de stockage temporaire permettant d'enregistrer rapidement des données en entrée ou en sortie.

Un canal d'accès direct à la mémoire, appelé DMA (*Direct Memory Access* soit *Accès direct à la mémoire*), a ainsi été défini pour y remédier.

Le canal DMA désigne un accès à un emplacement de la mémoire vive (RAM) de l'ordinateur, repéré par une « adresse de début » (ou «RAM Start Address» en anglais) et une « adresse de fin ». Cette méthode permet à un périphérique d'emprunter des canaux spéciaux qui lui donnent un accès direct à la mémoire, sans faire intervenir le microprocesseur, afin de le décharger de ces tâches.

Un ordinateur de type PC possède 8 canaux DMA. Les quatre premiers canaux DMA ont une largeur de bande de 8 bits tandis que les DMA 4 à 7 ont une largeur de bande de 16 bits.

Les canaux DMA sont généralement assignés comme suit :

DMA0 - libre

DMA1 - (carte son)/ libre

DMA2 - contrôleur de disquettes

DMA3 - port parallèle (port imprimante)

DMA4 - contrôleur d'accès direct à la mémoire

(renvoi vers DMA0)

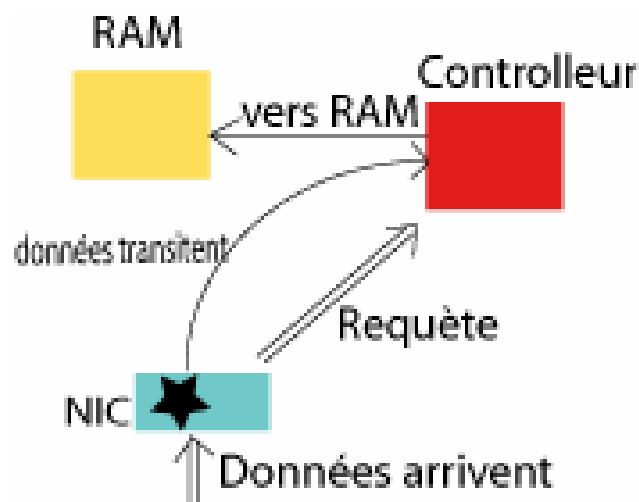
DMA5 - (carte son)/ libre

DMA6 - (SCSI)/ libre

DMA7 - disponible

#### Fonctionnement du DMA :

1. Les données entrent dans la carte réseau depuis le réseau
2. Le processeur de la carte réseau envoie une interruption au contrôleur de DMA.
2. Le contrôleur de DMA prend possession du bus de données du micro processeur.
2. Le processeur de l'ordinateur cède son bus en continuant son traitement de données et le processeur de la carte réseau copie les données de la carte réseau sur la RAM pour leur traitement.



#### d) L'adresse de base E/S

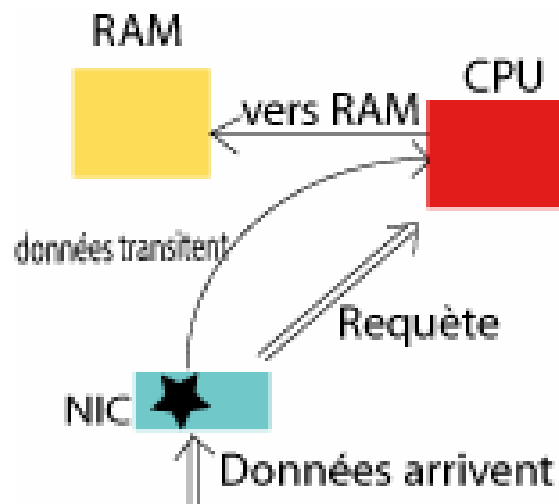
Les périphériques ont parfois besoin d'échanger des informations avec le système, c'est pourquoi des adresses mémoire leur sont assignées pour l'envoi et la réception de données. Ces adresses sont appelées «adresses de base» (les termes suivants sont également parfois utilisés : «ports d'entrée/sortie», «ports d'E/S», «adresse d'E/S», «adresses de ports d'E/S», «ports de base», ou en anglais *I/O address* qui signifie «*Input/Output Address*», littéralement «*Adresse d'entrée - sortie*»). C'est par l'intermédiaire de cette adresse de base que le périphérique peut communiquer avec le système d'exploitation. Il ne peut donc exister qu'une adresse de base unique par périphérique. Voici une liste de quelques adresses de base courantes :

060h - clavier  
170h/376h - contrôleur IDE secondaire  
1F0h/3F6h - contrôleur IDE primaire  
220h - carte son  
300h - carte réseau  
330h - carte adaptatrice SCSI  
3F2h - contrôleur de lecteur de disquettes  
3F8h - COM1  
2F8h - COM2  
3E8h - COM3  
2E8h - COM4  
378h - LPT1  
278h - LPT2

Tous ces éléments sont toutefois transparents pour l'utilisateur moyen, c'est-à-dire qu'il n'a pas à s'en préoccuper.

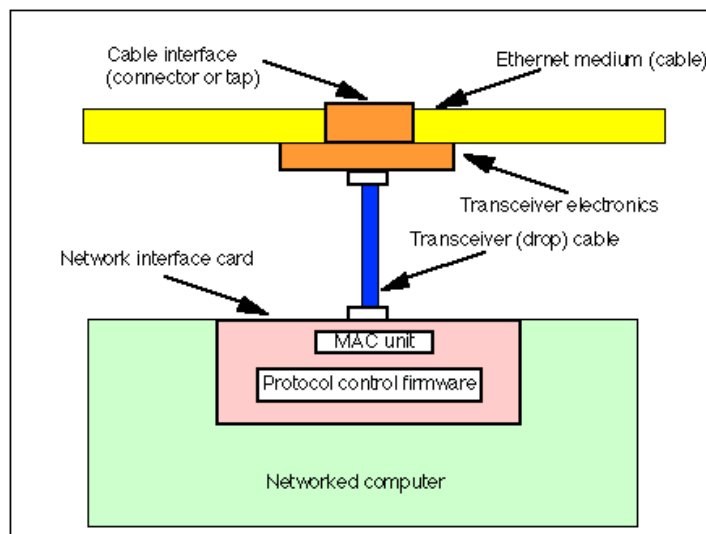
#### Fonctionnement du I/O :

1. Les données entrent dans la carte réseau depuis le réseau
2. Le processeur de la carte réseau envoie une interruption au Processeur
3. Le processeur interrompt son travail en cours et traite la requête.
4. Le processeur prend les données de la carte réseau et les fait transiter lui-même vers la Ram pour les traiter.



### e) Le transceiver

*Le transceiver* : transforme les données parallèles en donnée série. Il transforme les données arrivant par le câble et les transforme en donnée que la carte puisse traiter (séries de bits).



### f) Le Plug-and-Play

On parle de « Plug-and-Play » lorsqu'il suffit de brancher une extension pour qu'elle soit opérationnelle. Le système reconnaît ces nouvelles extensions, et l'utilisateur n'a plus de paramétrage à faire (en théorie). C'est en fait une norme dévoilée par Microsoft et Intel en 1991 (alors que sur les Macs, on connaît depuis des années...). Windows 95 était dit Plug and Play à sa sortie : c'est pourquoi il ne reconnaissait pas la plupart des lecteurs de CD-ROM. On pouvait toujours essayer de lui brancher autre chose qu'un Mitsumi, un Panasonic ou un Sony en 1996...

*Comment fonctionne-t-il derrière cette façade ?*

Voici une explication très simple de la façon dont fonctionne le *PnP*. Le programme de configuration *PnP* (éventuellement un programme du BIOS) recherche tous les périphériques *PnP* et demande à chacun les ressources du bus dont il a besoin. Ensuite, il regarde les ressources du bus (IRQs, etc.) qu'il doit attribuer. Bien sûr, s'il y a des ressources du bus réservées par des périphériques (anciens) non *PnP* (dont il a connaissance), il ne les attribue pas. Puis il utilise un certain critère (non précisé dans les spécifications *PnP*) pour attribuer les ressources de façon à ce qu'elles n'entrent pas en conflit et que tous les périphériques obtiennent ce dont ils ont besoin. Il indique alors à chaque périphérique physique quelles ressources du bus lui ont été affectées et chacun se configure alors pour n'utiliser que les seules ressources du bus qui lui ont été affectées.

Par exemple, supposons qu'une carte ait besoin d'une interruption (d'un numéro d'interruption) et de 1 MB de mémoire partagée. Le programme *PnP* lit cette requête dans la carte. Il attribue alors le numéro d'interruption 5 (IRQ 5) et un méga-octet d'espace mémoire à partir de l'adresse 0xe9000000. Ce n'est pas toujours aussi simple car la carte peut utiliser uniquement certains numéros d'interruption (seulement pour ISA) ou n'accepter qu'un certain domaine d'adressage. Les détails sont différents pour les bus ISA et PCI, les choses étant plus complexes pour le bus ISA

Le logiciels *PnP* peut utiliser quelques raccourcis. L'un d'entre eux consiste à garder une trace de la manière dont il a assigné les ressources du bus lors de la dernière configuration (lors de la dernière utilisation de l'ordinateur) et la réutiliser. Windows9x et les BIOS PNP le font mais ce n'est pas le cas du Linux standard. Windows9x enregistre ces informations dans ses "Registres" sur le disque dur et un BIOS PnP le fait dans la mémoire non volatile de votre PC (connu sous le nom d' ESCD; voir La Base de données ESCD du BIOS).

Sous Linux, c'est le règne du "chaque périphérique pour lui-même" et il n'existe aucun registre centralisé des affectations de ressources. Certains pilotes de périphériques enregistrent la dernière configuration qu'ils ont utilisé et la réutilisent à la prochaine remise en route de l'ordinateur. Implicitement, ils considèrent que le reste du matériel n'aura pas besoin d'utiliser ses ressources du bus.

Si les périphériques se souvenaient de leur configuration précédente, il n'y aurait aucun matériel pour les reconfigurer au prochain démarrage, mais ils semblent oublier leur configuration lorsque l'on stoppe l'alimentation. Certains périphériques ont une configuration par défaut (mais pas nécessairement la dernière utilisée). Le programme de configuration *PnP* doit être exécuté à chaque mise sous tension du PC. De même, si l'on ajoute un nouveau périphérique, celui-ci a besoin d'être configuré. L'allocation de ressources du bus à ce nouveau périphérique peut nécessiter d'en enlever à un périphérique existant et de donner à celui-ci des ressources du bus différentes qu'il pourra utiliser à la place.

### g) Transmission de données entre 2 cartes réseaux

Avant de transmettre des données sur le réseau, une carte émettrice et une carte réceptrice se mettent d'accord sur :

- La taille maximale des groupes de données à envoyer.
- Le volume des données à envoyer avant confirmation.
- Les intervalles temporels entre les transmissions partielles de données
- Le délai d'attente avant envoi d'une confirmation
- La quantité de données que peut contenir chaque carte avant débordement.
- La vitesse de transmission des données.

Si une carte plus récente, plus rapide, doit communiquer avec une carte plus ancienne, les deux cartes doivent s'entendre sur une vitesse de transmission commune.

Chaque carte communique ses caractéristiques puis accepte ou modifie ses propres paramètres.

Lorsque tous les paramètres de connexion sont réglés, les deux cartes commencent à envoyer et à recevoir des données.

### Les techniques de transmission en informatique

Il existe principalement deux techniques ou modes de transmission des signaux qui sont utilisés en informatique :

- La transmission en bande de base (BASEBAND) est numérique
- La transmission en large bande (BROADBAND) est analogique

La transmission d'un signal est différenciée selon que l'émetteur et le récepteur fonctionnent ou pas au même rythme :

- La transmission asynchrone transfère des unités de données les une après les autres. Chaque unité (un octet égal à un caractère alphanumérique par exemple) est encadrée par un bit de START et un bit de STOP.
- La transmission synchrone transfère les données par paquets. Les données sont expédiées en groupe et sont également encadrées. Un paquet (contenant 1500 octets de données par exemple) est constitué d'une tête et d'une queue.

### La transmission en bande de base(BASEBAND)

Les caractéristiques d'une transmission en bande de base (BASEBAND) :

- Transporte les signaux numériques sur une unique fréquence
- Transporte les signaux sous la forme d'impulsions discrètes, c'est à dire qu'il y a des interruptions entre chaque impulsion.
- Transporte les signaux électriques ou lumineux
- Transporte un seul signal à la fois, la transmission en bande de base occupe toute la bande passante (toute la capacité du canal de communication), le câble constitue un canal unique
- Transporte les signaux dans les deux sens, la transmission est bidirectionnelle

Certains équipements d'un réseau en bande de base transmettent les signaux numériques dans les deux sens simultanément.

A mesure qu'il parcourt un câble, le signal électrique diminue progressivement en intensité et peut être l'objet de distorsion. Un signal trop faible ou déformé risque de ne pas être reconnu ou d'être mal interprété par son destinataire ; c'est pourquoi des répéteurs sont installés sur des câbles trop longs afin de rétablir la force et la définition du signal d'origine.

### La transmission en large de bande(BROADBAND)

La transmission en large de bande (BROADBAND) :

- Transporte les signaux analogiques sur une plage de fréquence
- Transporte les signaux continus, c'est à dire qu'il n'y a pas d'interruption, c'est seulement la hauteur de la fréquence qui varie.
- Transporte les ondes électromagnétiques ou optiques
- Transporte éventuellement plusieurs signaux simultanément (plusieurs transmissions analogiques peuvent cohabiter en même temps sur le même câble si la bande passante est suffisante, le câble propose alors plusieurs canaux de transmission)
- Transporte les signaux dans un seul sens, le flux est toujours unidirectionnel

Une des spécificités de la transmission en large de bande est que plusieurs canaux peuvent fonctionner simultanément sur le même support. C'est ce mode de transmission qu'utilise par exemple la télévision par câble. La bande passante est divisée en plage, et chaque plage constitue un canal de communication indépendant. Dans un réseau informatique, les ordinateurs qui communiquent sur une certaine fréquence doivent être configurés pour n'utiliser que la plage qui leur a été attribuée.

Les systèmes en large de bande ont recourt à des amplificateurs pour régénérer le signal analogique.

### Les deux méthodes pour disposer de deux canaux de transmission en large de bande

Le système en large de bande est unidirectionnel, il doit donc posséder deux canaux afin de véhiculer les signaux dans les deux sens (ainsi, les ordinateurs d'un réseau seront en mesure d'émettre et de recevoir).

Il existe deux façons de disposer de deux canaux :

- La configuration en large de bande avec subdivision médiane. La bande passante est divisée en deux. Une partie de la bande passante sert pour recevoir et l'autre partie pour émettre.
- La configuration en large de bande avec deux câbles distincts. L'un des câbles sert pour recevoir, l'autre pour émettre.

## **6. Caractéristiques d'un réseau**

Les réseaux locaux sont des infrastructures complexes et pas seulement des câbles entre stations de travail. Et, si l'on énumère la liste des composants d'un réseau local, on sera surpris d'en trouver une quantité plus grande que prévue :

\* Le **câblage** constitue l'infrastructure physique, avec le choix entre paire téléphonique, câble coaxial(UTP, FTP) et fibre optique. Ce choix détermine le type de concentrateurs (switch, HUB) du réseau. Ceux-ci constituent les nœuds internes dans le cas de réseaux en étoile. (détaillé dans structure hardware qui suit)

\* La **méthode d'accès** décrit la façon dont le réseau arbitre les communications des différentes stations sur le câble: ordre, temps de parole, organisation des messages. Elle dépend étroitement de la topologie et donc de l'organisation spatiale des stations les unes par rapport aux autres. La méthode d'accès est essentiellement matérialisée dans les cartes d'interfaces, qui connectent les stations au câble.

\* Les **protocoles** de réseaux sont des logiciels qui "tournent" à la fois sur les différentes stations et leurs cartes d'interfaces réseaux, c'est le langage de communication. Pour que deux structures connectées sur le réseau, ils doivent "parler" le même protocole.

\* Le **système d'exploitation** du réseau (ou NOS pour Network Operating System), souvent nommé gestionnaire du réseau, réside dans les différentes stations du réseau local. Il fournit une interface entre les applications de l'utilisateur et les fonctions du réseau local auxquelles il fait appel par des demandes à travers la carte d'interface.

\* Le **serveur de fichier** stocke et distribue les fichiers de programmes ou les données partageables par les utilisateurs du réseau local. Il résulte d'une combinaison de matériel et de logiciel qui peut être spécifique. Ils sont également utilisés comme serveurs d'impression.

\* Le type de **serveur utilisé** (serveur d'impression, de fichier ou d'application)est spécifique et permet d'utiliser un programme spécifique à partir de toutes les stations connectées. Ces serveurs sont nettement plus musclés. Cette solution est surtout utilisée en MainFrame. Si elle augmente la sécurité (sauvegarde complète sur 1 ordinateur), le serveur envoie en permanence les parties de programme et données vers chaque station, ce qui augmente nettement le trafic réseau. Les serveurs de ce type sont multiprocesseurs. Le programme doit être conçu pour comme application centralisé. Ces programmes sont généralement de grosses bases de données.

\* Le ou les **clients** sont des ordinateurs ou périphériques connectés qui utilisent les ressources des serveur de fichiers, d'impression ou de programmes. Ils ne partagent pas leurs ressources.

\* Le **système de sauvegarde** est un élément indispensable qui fonctionne de diverses manières soit en recopiant systématiquement tous les fichiers du ou des serveurs, soit en faisant des sauvegardes régulières, éventuellement automatisées.

\* Un **pont**, un **routeur** ou **passerelle** constituent les moyens de communication qui permettent à un de ses utilisateurs de "sortir" du réseau local pour atteindre d'autres réseaux locaux ou des serveurs distants.

\* Le **système de gestion et d'administration** du réseau envoie les alarmes en cas d'incidents, comptabilise le trafic, mémorise l'activité du réseau et aide le superviseur à prévoir l'évolution de son réseau.

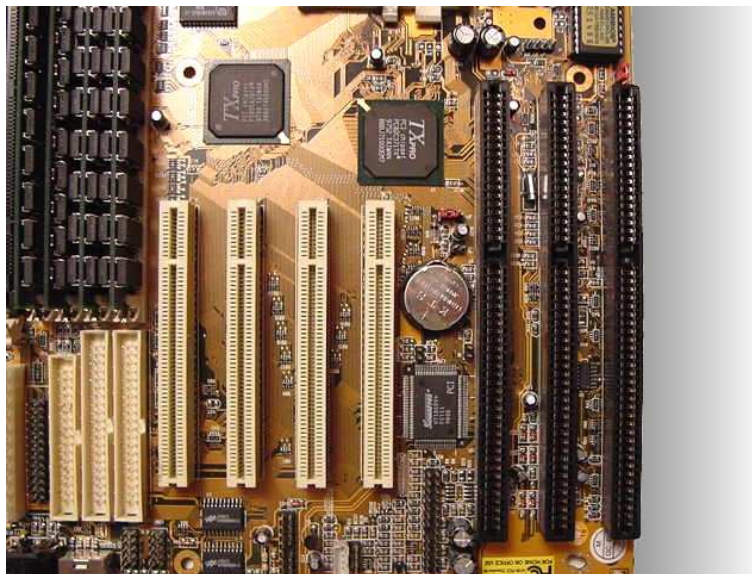
## **7. Structure hardware**

### ➤ L'interface : les bus

On appelle bus interne (parfois Bus de périphérique ou bus d'expansion) les connecteurs de l'ordinateur permettant d'ajouter des cartes d'extension (périphériques). Il existe différents types de bus internes normalisés caractérisés par :

- leur forme
- le nombre de broches de connexion
- le type de signaux (fréquence, données, etc.)

Presque toutes les cartes réseaux sont désormais sur bus PCI. Ce bus a l'avantage de facilité l'installation de la carte (Plug And Play) et est surtout moins gourmand en ressources processeurs que le bus ISA. La disparition des ports ISA confirme ce passage vers le PCI et la simplification du partage des ressources par cette technologie. Dès à présent la plupart des carte mère intègre une carte réseau (en Gigabits) cela permet de libérer les port PCI pour d'autre périphérique (carte son, carte d'acquisition)



PCI : 4connecteurs blancs    ISA : 3connecteurs noirs

### Le bus ISA

La version originale du bus ISA (*Industry Standard Architecture*), apparue en 1981 avec le PC XT, était un bus d'une largeur de 8 bits cadencé à une fréquence de 4,77 MHz.

En 1984, avec l'apparition du PC AT (processeur *Intel 286*), la largeur du bus est passée à 16 bits et la fréquence successivement de 6 à 8 MHz, puis finalement 8,33 MHz, offrant ainsi un débit théorique maximal de 16 Mo/s (en pratique seulement 8 Mo/s dans la mesure où un cycle sur deux servait à l'adressage). Cette évolution du bus ISA a été baptisée EISA (pour *Extended Industry Standard Architecture*).

Le bus ISA permettait le bus mastering, c'est-à-dire qu'il permettait de communiquer directement avec les autres périphériques sans passer par le processeur. Une des conséquences du *bus mastering* est l'accès direct à la mémoire (DMA, pour *Direct Memory Access*). Toutefois le bus ISA ne permettait d'adresser que les 16 premiers méga-octets de la mémoire vive.

Jusqu'à la fin des années 1990 le bus ISA équipait la quasi-totalité des ordinateurs de type PC, puis il a été progressivement remplacé par le bus PCI, offrant de meilleures performances.

Connecteur ISA 8 bits :



Connecteur ISA 16 bits :

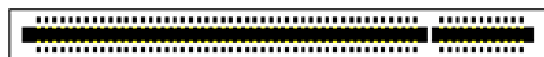


### Le bus PCI

Le bus PCI (*Peripheral Component Interconnect*) a été mis au point par Intel en 1992. Contrairement au bus VLB il ne s'agit pas à proprement parler d'un bus local mais d'un bus intermédiaire situé entre le bus processeur (*NorthBridge*) et le bus d'entrées-sorties (*SouthBridge*).

Le bus PCI possède une largeur de 32 bits et est cadencé à 33 MHz dans sa version originale, ce qui lui permet d'offrir un débit de 132 Mo/s.

Les connecteurs PCI sont généralement présents sur les cartes mères au nombre de 3 ou 4 au minimum et sont en général reconnaissables par leur couleur blanche (normalisée) :



### ➤ Les connecteurs

Il existe 2 types de connecteurs : RJ45 et BNC.

La connectique BNC implique le réseau soit un poste à poste. C'est à dire que la 1er machine est connectée à la 2nd, la 2nd à la 3eme et ainsi de suite. Il faut donc des bouchons terminateurs en début de chaîne ou en fin de chaîne.

La connectique RJ45 implique la présence d'un concentrateur (hub ou l'utilisation d'un câble croisé dans une connexion simple entre 2 machines). Chaque machine(ici câble droit) est reliée au concentrateur qui se charge de gérer les échanges de données entre chaque machine.

Le désavantage du BNC par rapport au RJ45 est que lorsque une machine se déconnecte du réseau, tout le réseau plante. Au delà de 3 machines, il vaut mieux utiliser la connectique RJ45 avec un hub.

Certains hubs comporte un connecteur BNC et donc on peut relier un réseau poste à poste au hub. Etant donné sa faible vitesse et d'utilisation du câble le BNC est de moins utilisé.



### La vitesse...

Il existe deux types de cartes : 10Mps et 100Mps. Les premières ont un débit d'environ 1mo/s et les secondes 10mo/s. Seulement, pour supporter un tel débit de 10mo/s, il faut que la machine puisse suivre. Il existe aussi des cartes qui gère les 2 protocoles : 10/100Mps.



Les cartes 10Mps ont une double connectique RJ45 et BNC alors que les 10/100Mps, 100Mps et même les carte Gigabits n'ont que la connectique RJ45.

De la vitesse découle un diamètre maximum du réseau. En général, on se trouve bien largement au dessous de ce maximum dans tous les réseaux domestiques.

Exemple concret du diamètre en fonction de la vitesse :

En négligeant le retard introduit par les cartes, répéteurs et hubs, calculer le diamètre du réseau (en mètres) pour Ethernet 10 M bit/s, 100 M bit/s et 1 G bit/s.

Vitesse de déplacement dans le support : 200 000 km/s.

→ Ethernet 10 M bit/s :

512 bits passent en 51,2 microseconde à 10 M bit/s

Pendant ce temps ils parcourent  $200 * 51,2 = 10\,240$  m

Diamètre :  $10\,240 / 2 = 5\,120$  m

Retenons 5 000 m maximum, mais en général, on est largement en dessous.

→ Ethernet 100 M bit/s

Même raisonnement : environ 500 m ( maximum ).

→ Ethernet 1 G bit/s

4096 bits passent en 4,096 microseconde à 1 G bit/s

Pendant ce temps ils parcourent  $200 * 4,096 = 819,2$  m

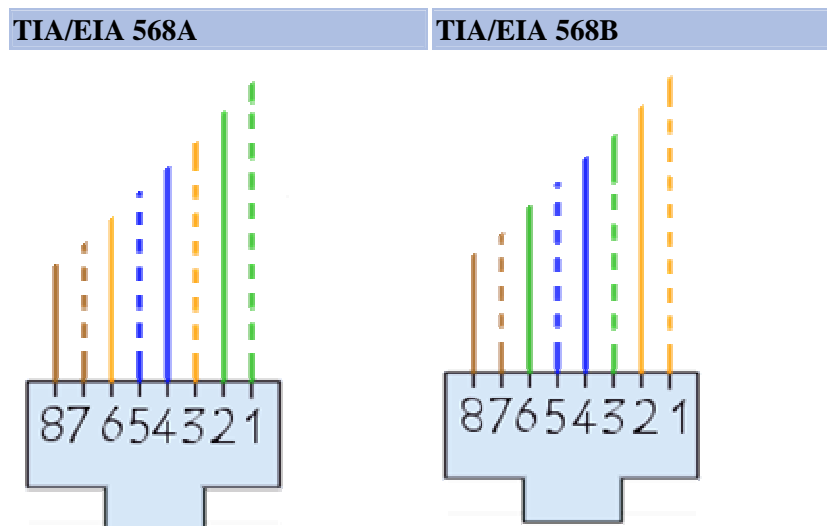
Diamètre :  $819 / 2 = 410$  m : environ 400 m ( maximum ).

### ➤ Le câblage

Le câblage des réseaux locaux tend aujourd'hui à se banaliser, et à ne pas se distinguer du câblage informatique et téléphonique général de l'entreprise. Trois médias sont aujourd'hui utilisés dans les réseaux locaux:

\* La *paire torsadée téléphonique*, peu chère, assez facile à poser, elle est aujourd'hui le support le plus répandu pour les réseaux locaux. Elle est souvent reprise sous le terme réseau Ethernet ou réseau RJ45

Les câbles utilisés sont appelés *paires torsadées* (en anglais *twisted pairs*) car ils sont constitués de 4 paires de fils torsadés. Chaque paire de fils est constituée d'un fil de couleur unie et d'un fil possédant des rayures de la même couleur. Il est fortement recommandé d'utiliser du câble de catégorie 5 d'une longueur minimale de 3 mètres et d'une longueur maximale de 90 mètres. Il existe deux standards de câblage différant par la position des paires orange et verte, définis par le *Electronic Industry Association/Telecommunications Industry Association* :



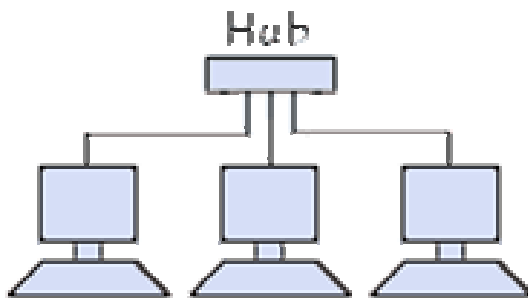
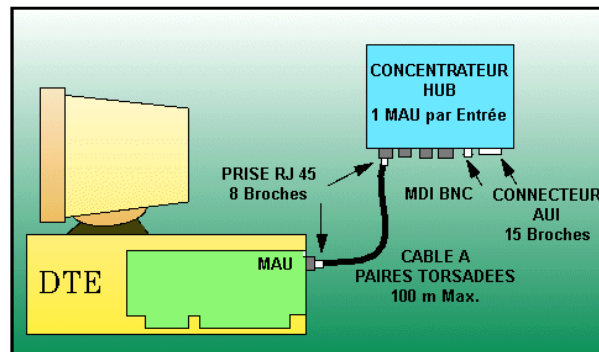
Connecteur RJ45 sur une prise mâle vue de face, contacts vers le haut.

Le connecteur 1 est à gauche sur une prise femelle (carte réseau ou bien prise murale) et à droite sur une prise mâle, connecteur vers soi, contacts vers le haut !

### Intérêt d'un câble droit

La connectique RJ45 sert normalement à connecter les ordinateurs par l'intermédiaire d'un hub (en français *concentrateur*, un boîtier de répartition sur lequel viennent se connecter les câbles RJ45 en provenance des ordinateurs du réseau local) ou d'un commutateur (en anglais *switch*).

#### ETHERNET 10 BASE-T



Lorsqu'un ordinateur est connecté à un hub ou à un switch, le câble utilisé est appelée *câble droit* (en anglais *patch cable*), ce qui signifie qu'un fil relié à la prise 1 d'un côté est relié à la prise 1 de l'autre côté. La norme de câblage généralement utilisée pour réaliser des câbles droits est la norme *TIA/EIA T568A*, cependant il existe des câbles droits selon la norme *TIA/EIA T568B* (seules les couleurs de

certains fils changent, cela n'a aucune incidence sur le fonctionnement dans la mesure où les fils sont reliés de la même façon).

### Intérêt d'un câble croisé

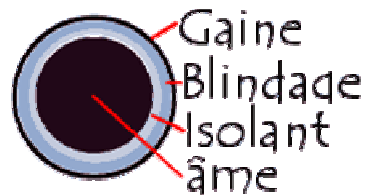
L'utilisation d'un hub est très utile dans le cas de la connexion de nombreux ordinateurs, et est nettement plus rapide qu'une connexion avec du câble coaxial. Toutefois, pour connecter ensemble deux machines il existe une technique permettant d'éviter l'utilisation d'un hub.

Cette technique consiste à utiliser un câble croisé (en anglais *cross cable* ou *crossover*), un câble dont deux fils se croisent. La norme recommandée pour ce type de câble est la norme *TIA/EIA T568A* pour une des extrémités, la norme *TIA/EIA T568B* pour l'autre. Ce type de câble s'achète bien évidemment dans le commerce, mais il est très facile à réaliser soi-même.

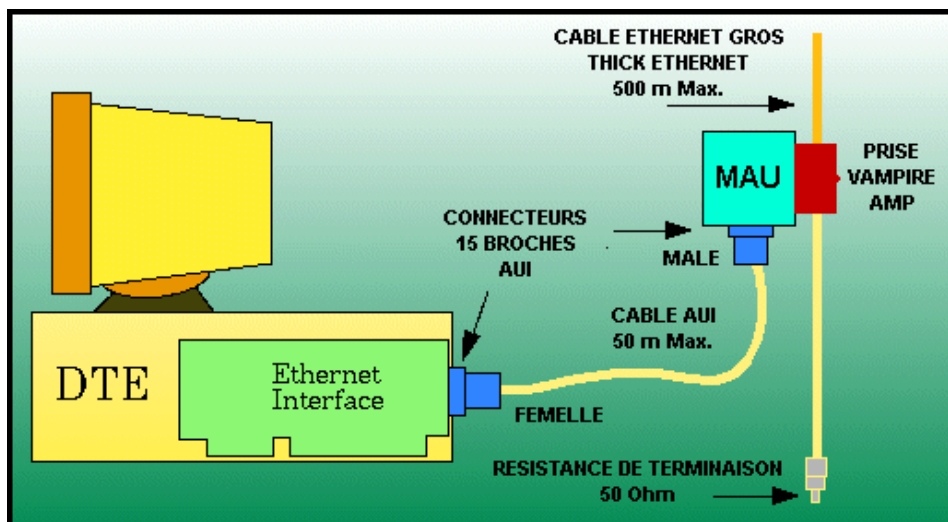
\* Le *câble coaxial*, nettement plus cher, est en perte de vitesse après avoir été le support par excellence des premiers réseaux locaux qui fonctionnaient en mode large bande (bande passante découpée en plages de fréquence, chacune étant attribuée à un canal). Aujourd'hui, la plupart des réseaux locaux fonctionnant en bande de base (toutes les stations émettent sur un même canal occupant la totalité de la bande passante), le câble coaxial est moins nécessaire et on l'emploie presque uniquement pour l'interconnexion de différents réseaux locaux.

La gaine permet de protéger le câble de l'environnement extérieur. Elle est habituellement en caoutchouc (parfois en Chlorure de polyvinyle (PVC), éventuellement en téflon)

Le blindage (enveloppe métallique) entourant les câbles permet de protéger les données transmises sur le support des parasites (autrement appelé bruit) pouvant causer une distorsion des données. L'isolant entourant la partie centrale est constitué d'un matériau diélectrique permettant d'éviter tout contact avec le blindage, provoquant des interactions électriques (court-circuit). L'âme, accomplissant la tâche de transport des données, est généralement composée d'un seul brin en cuivre ou de plusieurs brins torsadés.



### ETHERNET GROS - 10 BASE-5 -



**MAU** : Media Adapter Unit : réalise les opérations physiques d'échange de données entre la carte et le câble.

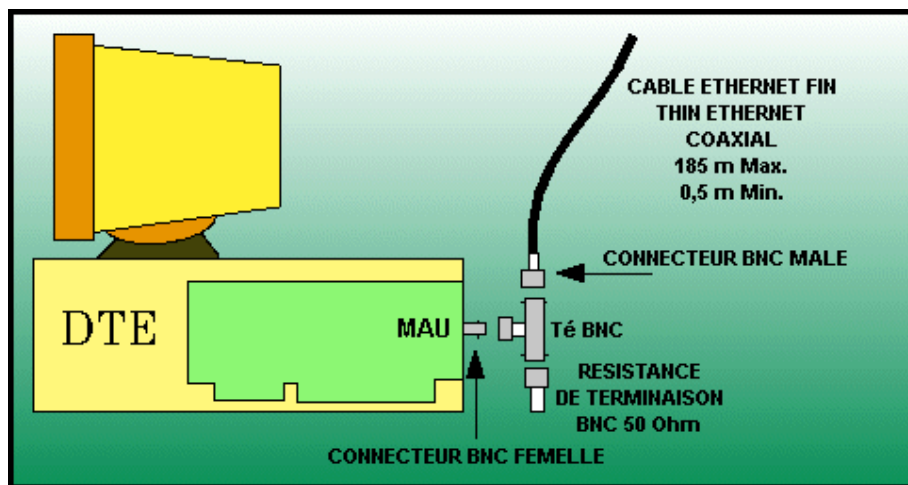
Maximum 100 MAU par segment espacées au moins de 2,5 m.

**Prise Vampire** : prise prenant contact à la fois avec la tresses externe du câble coaxial et son conducteur central.

Elle perce pour cela la gaine isolante du câble.

**DTE** : Data Terminal Equipement : Equipement Terminal de Traitement des données : ETTD en France.

ETHERNET FIN 10 BASE-2



La carte d'interface possède une MAU - Média Access Unit - interne.  
Les "T" BNC permettent de joindre deux stations du réseau.  
Les tés des deux stations extrêmes doivent recevoir des résistances de terminaison, vendues sous le nom de "bouchons", pour éviter les réflexions de fin de ligne.

\* *La fibre optique*, encore nettement plus chère, permet des débits élevés et est insensible aux parasites et commence à faire une percée dans les réseaux locaux à gros besoins de bande passante (calcul technique, CAO), mais sert surtout pour interconnecter plusieurs réseaux locaux. La fibre optique est chère, fragile et fastidieuse à installer. Elle casse facilement sous l'effet de la torsion. La fibre optique possède néanmoins de nombreux avantages:

- Légèreté
  - Immunité au bruit
  - Faible atténuation
  - Tolère des débits de l'ordre de 100Mbps
  - Largeur de bande de quelques dizaines de mégahertz à plusieurs gigahertz (fibre monomode)
- Le câblage optique est particulièrement adapté à la liaison entre répartiteurs (liaison centrale entre plusieurs bâtiments, appelé backbone) car elle permet des connexions sur des longues distances (de quelques kilomètres à 60 km dans le cas de fibre monomode) sans nécessiter de mise à la masse. De plus ce type de câble est très sûr car il est extrêmement difficile de mettre un tel câble sur écoute. Le type de câble utilisé détermine la vitesse maximale de transmission des données, ainsi que le standard de connexion des réseaux. Dans le cas de la paire torsadée, on utilise du câble téléphonique. Néanmoins, ces câbles sont repris suivant leurs caractéristiques physiques (diamètre, isolant, longueur des torsades) dans différentes catégories ci-dessous:

Type de câble	Vitesse supportée	Type de réseau
Catégorie 1	Téléphonie	Téléphone
Catégorie 2	1 Mbps	Token-ring et téléphone
Catégorie 3	16 Mbps	Token-Ring et 10 base T
Catégorie 4	20 Mbps	10 Base T
Catégorie 5	100 Mbps	10BaseT et 100 Base TX
Catégorie 5e (catégorie 6)	1 Gbps	Giga Ethernet

Il existe 2 familles de câbles de paires torsadées. Les câbles blindés (**STP**: Shielded Twisted Pair) disposent d'une feuille d'aluminium pour faire écran. Les câbles **UTP** (Unshielded twisted Pair) n'en possèdent pas. Les plus courants sont les UTP.

## **8. Le wifi**

### **Pourquoi le WiFi ?**

La norme IEEE 802.11 (ISO/IEC 8802-11) est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom Wi-Fi (contraction de Wireless Fidelity, parfois notée à tort WiFi) correspond initialement au nom donné à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage (et pour des raisons de marketing) le nom de la norme se confond aujourd'hui avec le nom de la certification. Ainsi un réseau Wifi est en réalité un réseau répondant à la norme 802.11. Les matériels certifiés par la Wi-Fi Alliance bénéficient de la possibilité d'utiliser le logo suivant :



Grâce au Wi-Fi il est possible de créer des réseaux locaux sans fils à haut débit pour peu que la station à connecter ne soit pas trop distante par rapport au point d'accès. Dans la pratique le Wi-Fi permet de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) ou tout type de périphérique à une liaison haut débit (11 Mbps ou supérieur) sur un rayon de plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) à plusieurs centaines de mètres en environnement ouvert.

Ainsi des opérateurs commencent à irriguer des zones à fortes concentration d'utilisateurs (gares, aéroports, hôtels, trains, ...) avec des réseaux sans fils. Ces zones d'accès sont appelées "hot spots".

### **Présentation de la norme 802.11**

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

la couche physique (notée parfois *couche PHY*), proposant trois types de codages de l'information.

la couche liaison de données, constitué de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC)

La couche physique définit la modulation des ondes radio-électriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche *liaison de données* définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet et les règles de communication entre les différentes stations. La norme 802.11 propose en réalité trois couches physiques, définissant des modes de transmission alternatifs :

Couche Liaison de données (MAC)	802.2 802.11
Couche Physique (PHY)	DSSSFHSSInfrarouges

Il est possible d'utiliser n'importe quel protocole de haut niveau sur un réseau sans fil WiFi au même titre que sur un réseau ethernet.

### **Les différentes normes WiFi**

La norme *IEEE 802.11* est en réalité la norme initiale offrant des débits de 1 ou 2 Mbps. Des révisions ont été apportées à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physiques) ou bien préciser des éléments afin d'assurer

une meilleure sécurité ou une meilleure interopérabilité. Voici un tableau présentant les différentes révisions de la norme 802.11 et leur signification :

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

Il est intéressant de noter l'existence d'une norme baptisée «802.11b+». Il s'agit d'une norme propriétaire proposant des améliorations en terme de débits. En contrepartie cette norme souffre de lacunes en termes de garantie d'interopérabilité dans la mesure où il ne s'agit pas d'un standard IEEE.

➤ Techniques de transfert du wifi

**Les canaux de transmission**

On appelle *canal de transmission* une bande étroite de fréquence utilisable pour une communication. Dans chaque pays, le gouvernement est en général le régulateur de l'utilisation des bandes de fréquences, car il est souvent le principal consommateur pour des usages militaires. Toutefois les gouvernements proposent des bandes de fréquence pour une utilisation libre, c'est-à-dire ne nécessitant pas de licence de radiocommunication. Les organismes chargés de réguler l'utilisation des fréquences radio sont :

l'ETSI (European Telecommunications Standards Institute) en Europe

la FCC (Federal Communications Commission) aux Etats-Unis

le MKK (Kensa-kentei Kyokai) au Japon

En 1985 les Etats-Unis ont libéré trois bandes de fréquence à destination de l'Industrie, de la Science et de la Médecine. Ces bandes de fréquence, baptisées ISM (Industrial, Scientific, and Medical), sont les bandes 902-928 MHz, 2.400-2.4835 GHz, 5.725-5.850 GHz.

En Europe la bande s'étalant de 890 à 915 MHz est utilisée pour les communications mobiles (GSM), ainsi seules les bandes 2.400 à 2.4835 GHz et 5.725 à 5.850 GHz sont disponibles pour une utilisation radioamateur.

**Les technologies de transmission**

Les réseaux locaux radioélectriques utilisent des ondes radio ou infrarouges afin de transmettre des données. La technique utilisée à l'origine pour les transmissions radio est appelé transmission en bande étroite, elle consiste à passer les différentes communications sur des canaux différents. Les transmissions radio sont toutefois soumises à de nombreuses contraintes rendant ce type de transmission non suffisantes. Ces contraintes sont notamment :

Le partage de la bande passante entre les différentes stations présentes dans une même cellule.

La propagation par des chemins multiples d'une onde radio. Un onde radio peut en effet se propager dans différentes direction et éventuellement être réfléchié ou réfractés par des objets de l'environnement physique, si bien qu'un récepteur peut être amené recevoir à quelques instants d'intervalles deux mêmes informations ayant emprunté des cheminements différents par réflexions successives.

La couche physique de la norme 802.11 définit ainsi initialement plusieurs techniques de transmission permettant de limiter les problèmes dus aux interférences :

- La technique de l'étalement de spectre à saut de fréquence,
- La technique de l'étalement de spectre à séquence directe,
- La technologie infrarouge.

**La technique à bande étroite**

La technique à bande étroite (narrow band) consiste à utiliser une fréquence radio spécifique pour la transmission et la réception de données. La bande de fréquence utilisée doit être aussi petite que possible afin de limiter les interférences sur les bandes adjacentes.

**Les techniques d'étalement de spectre**

La norme IEEE 802.11 propose deux techniques de modulation de fréquence pour la transmission de données issues des technologies militaires. Ces techniques, appelées étalement de spectre (en anglais spread spectrum) consistent à utiliser une bande de fréquence large pour transmettre des données à faible puissance. On distingue deux techniques d'étalement de spectre :

La technique de l'étalement de spectre à saut de fréquence,

La technique de l'étalement de spectre à séquence directe

### La technique de saut de fréquence

La technique FHSS (Frequency Hopping Spread Spectrum, en français étalement de spectre par saut de fréquence ou étalement de spectre par évation de fréquence) consiste à découper la large bande de fréquence en un minimum de 75 canaux (hops ou sauts d'une largeur de 1MHz), puis de transmettre en utilisant une combinaison de canaux connue de toutes les stations de la cellule. Dans la norme 802.11, la bande de fréquence 2.4 - 2.4835 GHz permet de créer 79 canaux de 1 MHz. La transmission se fait ainsi en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (d'environ 400 ms), ce qui permet à un instant donné de transmettre un signal plus facilement reconnaissable sur une fréquence donnée.

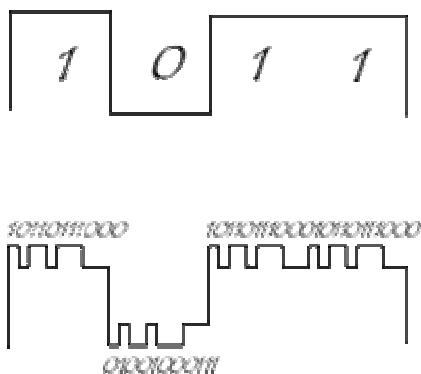
L'étalement de spectre par saut de fréquence a originalement été conçu dans un but militaire afin d'empêcher l'écoute des transmissions radio. En effet, une station ne connaissant pas la combinaison de fréquence à utiliser ne pouvait pas écouter la communication car il lui était impossible dans le temps imparti de localiser la fréquence sur laquelle le signal était émis puis de chercher la nouvelle fréquence.

Aujourd'hui les réseaux locaux utilisant cette technologie sont standards ce qui signifie que la séquence de fréquences utilisées est connue de tous, l'étalement de spectre par saut de fréquence n'assure donc plus cette fonction de sécurisation des échanges. En contrepartie, le FHSS est désormais utilisé dans le standard 802.11 de telle manière à réduire les interférences entre les transmissions des diverses stations d'une cellule.

### Étalement de spectre à séquence directe

La technique DSSS (Direct Sequence Spread Spectrum, étalement de spectre à séquence directe) consiste à transmettre pour chaque bit une séquence Barker (parfois appelée bruit pseudo-aléatoire ou en anglais pseudo-random noise, noté PN) de bits. Ainsi chaque bit valant 1 est remplacé par une séquence de bits et chaque bit valant 0 par son complément.

La couche physique de la norme 802.11 définit une séquence de 11 bits (10110111000) pour représenter un 1 et son complément (01001000111) pour coder un 0. On appelle chip ou chipping code (en français puce) chaque bit encodé à l'aide de la séquence. Cette technique (appelée chipping) revient donc à moduler chaque bit avec la séquence barker.



Grâce au chipping, de l'information redondante est transmise, ce qui permet d'effectuer des contrôles d'erreurs sur les transmissions, voire de la correction d'erreurs.

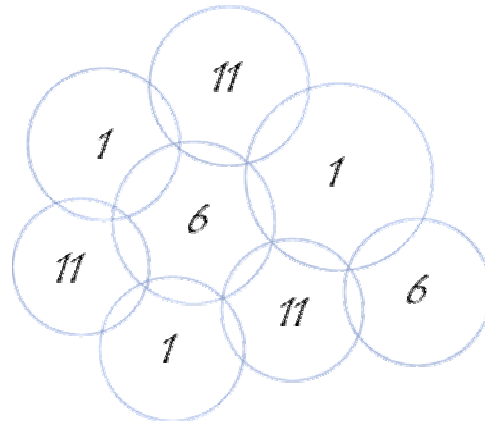
Dans le standard 802.11b, la bande de fréquence 2.400-2.4835 GHz (d'une largeur de 83.5 MHz) a été découpée en 14 canaux séparés de 5MHz, dont seuls les 11 premiers sont utilisables aux Etats-Unis.

Seuls les canaux 10 à 13 sont utilisables en France. Voici les fréquences associées aux 14 canaux :

Canal	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Fréquence (GHz)	2.412	2.417	2.422	2.427	2.432	2.437	2.442	2.447	2.452	2.457	2.462	2.467	2.472	2.484

Toutefois, pour une transmission de 11 Mbps correcte il est nécessaire de transmettre sur une bande de 22 MHz car, d'après le théorème de Shannon, la fréquence d'échantillonnage doit être au minimum égale au double du signal à numériser. Ainsi certains canaux recouvrent partiellement les canaux adjacents, c'est la raison pour laquelle des canaux isolés (les canaux 1, 6 et 11) distants les uns des autres de 25MHz sont généralement utilisés.

Ainsi, si deux points d'accès utilisant les mêmes canaux ont des zones d'émission qui se recoupent, des distorsions du signal risquent de perturber la transmission. Ainsi pour éviter toute interférence il est recommandé d'organiser la répartition des points d'accès et l'utilisation des canaux de telle manière à ne pas avoir deux points d'accès utilisant les mêmes canaux proches l'un de l'autre.



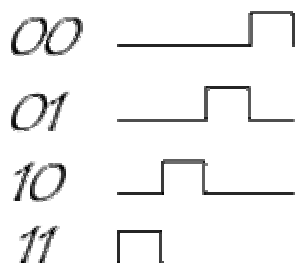
Le standard 802.11a utilise la bande de fréquence 5.15GHz à 5.35GHz et la bande 5.725 GHz à 5.825 GHz, ce qui permet de définir 8 canaux distincts d'une largeur de 20Mhz chacun, c'est-à-dire une bande suffisamment large pour ne pas avoir de parasitage entre canaux.

### La technologie infrarouge

Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon uni-directionnelle, soit en "vue directe" soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé.

Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé PPM (pulse position modulation).

La modulation PPM consiste à transmettre des impulsions à amplitude constante, et à coder l'information suivant la position de l'impulsion. Le débit de 1 Mbps est obtenu avec une modulation de 16-PPM, tandis que le débit de 2 Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles :



### Les techniques de modulation

Tandis que la radio classique utilise une modulation de fréquence (radio FM pour Frequency Modulation) ou bien une modulation d'amplitude (radio AM pour Amplitude Modulation), le standard 802.11b utilise une technique de modulation de phase appelée PSK pour Phase Shift Keying. Ainsi chaque bit produit une rotation de phase. Une rotation de 180° permet de transmettre des débits peu

élevés (technique appelé BPSK pour Binary Phase Shift Keying) tandis qu'une série de quatre rotations de 90° (technique appelé QPSK pour Quadrature Phase Shift Keying) permet des débits deux fois plus élevés.

### **Optimisations**

La norme 802.11b propose d'autres types d'encodage permettant d'optimiser le débit de la transmission. Les deux séquences Barker ne permettent de définir que deux états (0 ou 1) à l'aide de deux mots de 11 bits (compléments l'un de l'autre).

Une méthode alternative appelée CCK (complementary code keying) permet d'encoder directement plusieurs bits de données en une seule puce (chip) en utilisant 8 séquences de 64 bits. Ainsi en codant simultanément 4 bits, la méthode CCK permet d'obtenir un débit de 5.5 Mbps et elle permet d'obtenir un débit de 11 Mbps en codant 8 bits de données.

La technologie PBCC (Packet Binary Convolutionary Code) permet de rendre le signal plus robuste vis-à-vis des distorsions dues au cheminement multiple des ondes hertziennes. Ainsi la société Texas Instrument a réussi à mettre au point une séquence tirant avantage de cette meilleure résistance aux interférences et offrant un débit de 22Mbit/s. Cette technologie baptisée 802.11b+ est toutefois non conforme à la norme IEEE 802.11b ce qui rend les périphériques la supportant non compatibles avec les équipements 802.11b.

La norme 802.11a opère dans la bande de fréquence des 5 GHz, qui offre 8 canaux distincts, c'est la raison pour laquelle une technique de transmission alternative tirant partie des différents canaux est proposée. L'OFDM (Orthogonal Frequency Division Multiplexing) permet d'obtenir des débits théoriques de 54 Mbps en envoyant les données en parallèle sur les différentes fréquences. De plus la technique OFDM fait une utilisation plus rationnelle du spectre.

Technologie	Codage	Type de modulation	Débit
802.11b	11 bits (Barker sequence)	PSK	1Mbps
802.11b	11 bits (Barker sequence)	QPSK	2Mbps
802.11b	CCK (4 bits)	QPSK	5.5Mbps
802.11b	CCK (8 bits)	QPSK	11Mbps
802.11a	CCK (8 bits)	OFDM	54Mbps
802.11g	CCK (8 bits)	OFDM	54Mbps

## **9. Les 2 grands réseaux**

### L'ARPANET

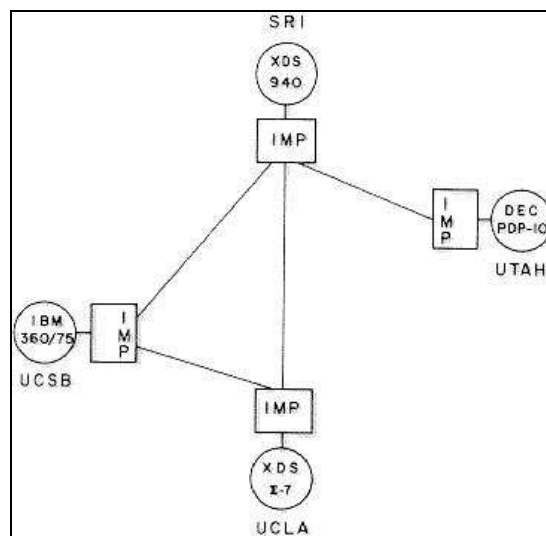
L'agence de recherche ARPA (Advanced Research Project Agency) crée en 1957 par le département américain de la défense a mis au point en 1969 le premier réseau mondial ARPANET qui ne dépend pas d'un centre névralgique qui pourrait être détruit en cas d'attaque nucléaire par les rouges. Le réseau a subi divers améliorations au cours des années 70 et 80, notamment l'introduction de plusieurs protocoles qui font que les serveurs se comprennent en tenant le même langage comme e-mail pour l'échange de courrier électronique ou ftp pour les échanges de fichiers.

En 1990 ARPANET cède définitivement la place à Internet et avec l'introduction des liens hypertextes en 1992, il ne cesse de devenir plus populaire et compte aujourd'hui plus de 30 Millions de serveurs dans le monde pour plus de 100 Millions d'utilisateurs.

1957 : Suite au lancement du premier Spoutnik par les Soviétiques, le président Dwight D. Eisenhower crée l'ARPA (Advanced Research Project Agency) au sein du DoD (Department of Defense) pour piloter un certain nombre de projets dans le but d'assurer aux USA la supériorité scientifique et technique sur leurs voisins Russes.

1967 : Lawrence G. Roberts, récemment arrivé à la tête du projet de réseau informatique à l'ARPA, publie ses "Plans pour le réseau ARPANET" au cours d'une conférence.

Le réseau ARPANET initial constitué de 4 ordinateurs est alors en fonctionnement fin 1969. Voici un schéma de l'époque représentant ce réseau.



Lors d'une interview, le professeur Kleinrock de l'UCLA raconta la première expérience réalisée avec ce réseau : se connecter à l'ordinateur de la SRI depuis celui de l'UCLA en tapant LOGIN :

*Nous avons appelé les gens de SRI par téléphone.*

*Nous avons alors tapé L puis demandé au téléphone "Vous voyez le L ?"*

*La réponse vint alors : "Oui, nous voyons le L"*

*Nous avons alors tapé O puis redemandé au téléphone "Vous voyez le O ?"*

*"Oui, nous voyons le O"*

*Nous avons alors tapé G et tout le système a crashé !!!*

Décembre 1970 : Le Network Working Group sous la direction de S. Crocker termine le protocole de communication entre ordinateurs pour le réseau ARPANET appelé Network Control Protocol ou NCP.



1984 : Mise en place du DNS (Domain Name Server) sur Internet. Jusque la, pour trouver une machine sur Internet, il fallait soit connaître son adresse numérique, soit tenir à jour un unique fichier texte contenant le nom et l'adresse numérique correspondante de toutes les machines de l'Internet, ce qui est rapidement devenu impossible avec la rapide croissance de ce réseau.

Octobre 1985 : Nombre de machines connectées sur **Internet** : **1961**

Février 1986 : Nombre de machines connectées sur **Internet** : **2308**

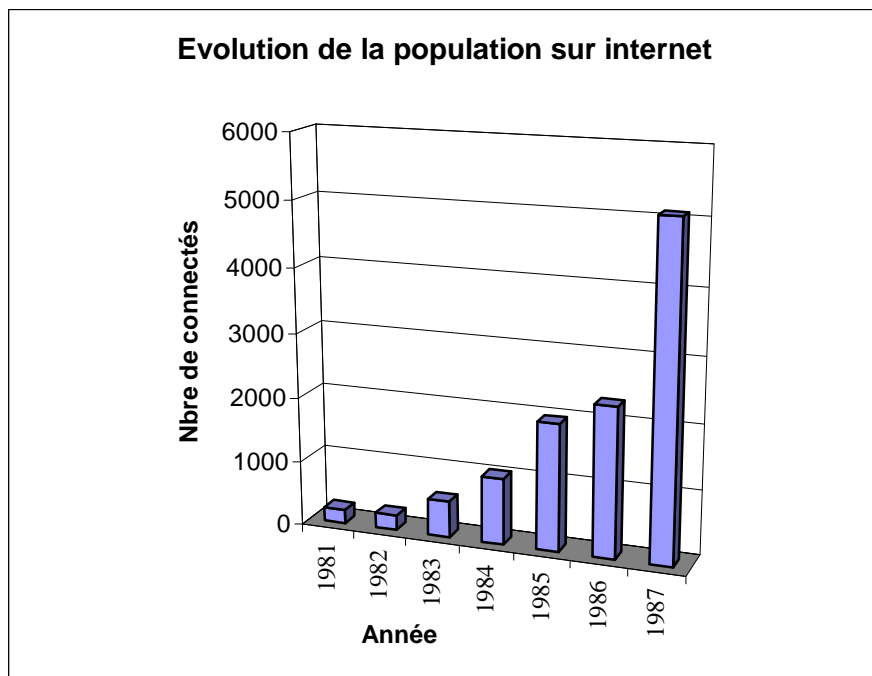
Novembre 1986 : Nombre de machines connectées sur **Internet** : **5089**

1990 : Internet s'impose finalement face à l'ARPANET

1992 : avec l'introduction des liens hypertextes.

Aujourd'hui : plus de 30 Millions de serveurs dans le monde pour plus de **100 Millions** d'utilisateurs.

Graphique de l'évolution du nombre de connectés aux débuts d'Internet

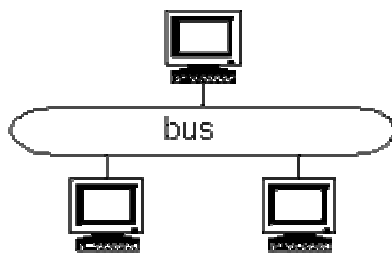


## 10. Topologies des réseaux

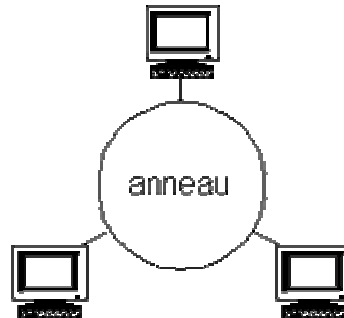
Dans le cas de notre liaison imprimante – PC, le câble centronix assurait le transport des données. Une liaison réseau est nettement plus complexe. Il ne suffit plus de connecter 2 appareils, mais bien plusieurs dans le sens large. Tout comme dans une liaison parallèle, les appareils à connecter sont reliés entre-eux par un câble (nous verrons également liaisons par infrarouge ou hertzienne). Avant d'étudier les différentes formes de liaisons, voyons les types de raccordements, appelés topologie.

Il y a trois types de topologie.

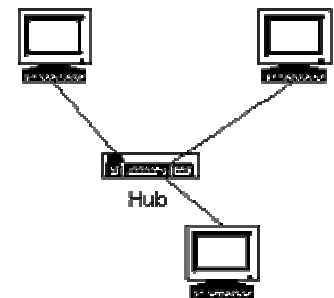
### Topologie en bus



### Topologie en anneau



### Topologie en étoile



→ Topologie en bus

Le bus, un segment central où circulent les informations, s'étend sur toute la longueur du réseau, et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinataire peut les récupérer. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.

L'avantage du bus est qu'une station en panne ne perturbe pas le reste du réseau. Elle est, de plus, très facile à mettre en place. Par contre, en cas de rupture du bus, le réseau devient inutilisable. Notons également que le signal n'est jamais régénéré, ce qui limite la longueur des câbles.

Cette topologie est utilisée dans les réseaux Ethernet 10 Base 2 et 10 Base 5.

→ Topologie en anneau

Développée par IBM, cette architecture est principalement utilisée par les réseaux Token Ring. Token Ring utilise la technique d'accès par « jeton ». Les informations circulent de stations en stations, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite...

Cette topologie permet d'avoir un débit proche de 90% de la bande passante. De plus, le signal qui circule est régénéré par chaque station. Par contre, la panne d'une station rend l'ensemble du réseau inutilisable. L'interconnexion de plusieurs anneaux n'est pas facile à mettre en œuvre. Enfin, cette architecture étant la propriété d'IBM, les prix sont élevés et la concurrence quasiment inexistante.

Cette topologie est utilisée par les réseaux Token Ring et FDDI.

Remarque: courant 2000, IBM a signalé qu'il ne suivrait plus de développement de circuits intégrés pour ce type de bus.

→ Topologie en étoile.

C'est la topologie la plus courante, notamment avec les réseaux Ethernet RJ45. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à toutes les autres machines (hub) ou à celle qui en est le destinataire (switch).

Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est anéanti. De plus, le débit pratique est moins bon que pour les autres topologies.

Cette topologie est utilisée par les réseaux Ethernet 10 et 100 Base T et par le 100 VG AnyLAN.

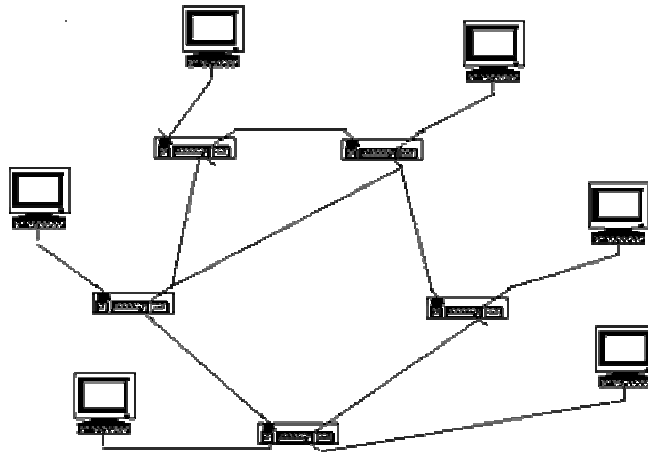
→ Topologie mixte.

Une topologie comme ci-dessus est malheureusement trop simpliste dans le cas de réseaux importants. Si une topologie en étoile est parfaite dans le cas d'un réseau limité géographiquement, un réseau mondial ne peut utiliser une liaison de ce type. La méthode utilisée est donc de relier des réseaux en étoile (par bâtiments par exemple) via des liaisons en bus (téléphoniques par exemple).

Dans la suite du cours, en nous intéressant aux connexions inter-réseaux, nous reverrons ce type de réseau mixte, en sachant que chaque partie du réseau est généralement en étoile.

→ Topologie maillée.

Les réseaux informatiques maillés (ici représentés par des ordinateurs) sont reliés par des routeurs qui choisissent la meilleure voie suivant plusieurs possibles. INTERNET est une topologie maillée, ceci garantit le mieux la stabilité en cas de panne d'un nœud mais est difficile à mettre en oeuvre, principalement au niveau du choix des routes à suivre pour transférer l'information. Ceci nécessite l'utilisation de routeurs intelligents.



## **11. Installation d'une carte réseau**

Débranchez tous les câbles de votre unité centrale, et posez la sur un espace de travail dégagé, ouvrez ensuite le capot (note: sur certains boîtier il est possible de n'ouvrir qu'un seul coté, dans ce cas c'est le côté gauche).

Pour commencer repérez un port **PCI** de libre (port blanc en bas de la carte mère), si besoin retirez le cache métallique du boîtier situé en face le connecteur, présentez la carte perpendiculairement au connecteur en faisant correspondre l'équerre de la carte avec l'ouverture située sur l'arrière du boîtier, puis appuyez doucement sur la carte pour l'insérer dans le connecteur (il faut parfois forcer légèrement).



Pour terminer vissez pour maintenir la carte.

Pour l'installation des pilotes il est conseillé de consulter la documentation fourni avec la carte ethernet.

Comment configurer une carte réseau.

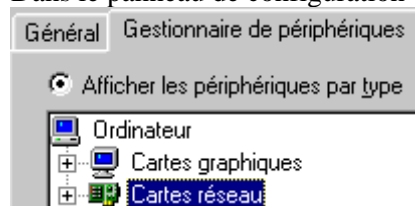
### **Installation matérielle**

La première chose à faire est d'ouvrir votre ordinateur et d'y insérer la carte réseau, qu'elle soit ISA ou bien PCI. Pour cela vous aurez besoin d'un tournevis cruciforme. Avant toutes choses débranchez l'alimentation, puis touchez le boîtier d'une main et le sol de l'autre, il ne vous reste plus qu'à trouver un emplacement de libre et d'y insérer la carte.


Si jamais des cavaliers (jumpers) sont présents sur la carte vérifiez leur utilité.

### **Installation logicielle de la carte**

Dans le panneau de configuration (système) double cliquez sur l'icône *ordinateur*



pour voir les ressources disponibles, car vous aurez besoin d'un IRQ et d'une plage d'entrée/sortie. Généralement l'IRQ 10 ou 12 et l'adresse 0240h sont libres...

Double-cliquez ensuite sur l'icône  Réseau du panneau de configuration, et faites *ajouter/carte*. Généralement les drivers par défaut de Windows 95 et Windows 98 fonctionnent parfaitement (mieux sous Windows 98), on les trouve dans *Novell/Carte compatible NE2000*. Si toutefois des drivers spécifiques pour Windows95 ou 98 sont présents sur la disquette fournie avec la carte réseau, essayez-les.

Lorsque cela vous est demandé entrez l'IRQ et le port I/O (Entrée/Sortie) que vous avez choisi précédemment.

Il vous faudra généralement relancer Windows, puis modifier à nouveau les paramètres car il ne les aura pas pris... puis relancer à nouveau.

Lorsque vous aurez enfin redémarré Windows allez voir dans le panneau de configuration. Si la carte apparaît avec un point d'exclamation jaune c'est qu'un conflit existe il vous faut alors modifier l'IRQ.



De nombreuses cartes nécessitent d'être en mode jumperless, c'est-à-dire qu'il faut les empêcher d'être Plug'N'Play. Pour cela il faut utiliser l'utilitaire DOS fourni sur la disquette (souvent appelé *setup.exe*) qui vous permettra de choisir le mode jumperless (sans cavalier) afin de pouvoir choisir les paramètres (IRQ, entrée-sortie) de votre choix. Il faudra bien sûr mettre les mêmes sous DOS et sous Windows...



A ce niveau la carte devrait être opérationnelle, il ne reste plus qu'à installer la partie logicielle, c'est-à-dire les protocoles qui vont permettre la communication entre les ordinateurs.

### Installation des protocoles


Les protocoles sont les éléments logiciels qui vont permettre la communication entre les ordinateurs.

Les trois principaux protocoles pour un réseau local sont:

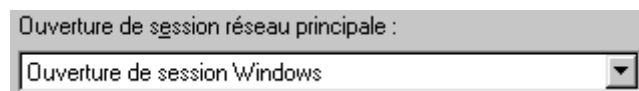
IPX-SPX: un protocole simple, utilisé notamment pour les jeux sous Windows 9x

NetBEUI: il est redondant avec IPX mais peut être nécessaire pour certains programmes

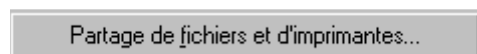
TCP/IP: le protocole utilisé sur Internet. Il vous sera nécessaire si vous décidez de relier votre réseau local à Internet

Pour installer chacun de ces protocoles, double-cliquez sur l'icône  Réseau du panneau de configuration, puis cliquez sur *ajouter/protocole*. Les protocoles ci-dessus sont disponibles sous le constructeur Microsoft.

Lorsque vous avez fini d'installer les différents protocoles, si jamais les ordinateurs connectés au réseau local tournent tous sous Windows 9x (et pas Windows NT) choisissez (toujours dans la fenêtre réseau) *Ouverture de session Windows* dans le menu déroulant intitulé *Ouverture de session réseau principale*



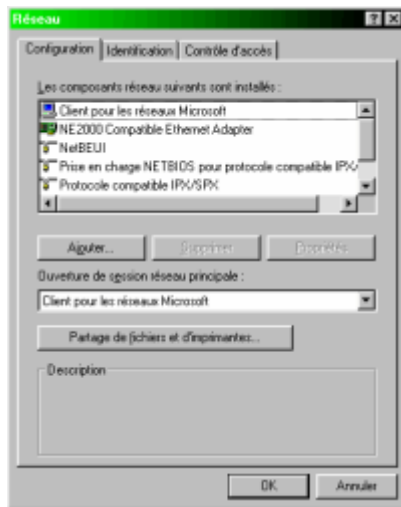
Cela vous évitera de devoir confirmer chaque ouverture de session Windows par un mot de passe. Enfin, si vous voulez que des personnes puissent accéder à certaines de vos ressources (fichiers, disques, répertoires, ou imprimantes), cliquez sur le bouton *Partage de fichiers et d'imprimantes*



puis cochez les choix qui vous intéressent.

Dans l'onglet *Identification* de la fenêtre *réseau* remplissez les champs relatifs à votre identification sur le réseau. Il faudra veiller à mettre le même nom de groupe de travail sur tous les ordinateurs du réseau local.

Il ne vous reste plus qu'à redémarrer Windows (à nouveau...)



Vous devriez normalement voir apparaître les composants réseau suivants (ainsi que d'autre éventuellement, notamment si vous possédez un modem...):

Client pour les réseaux Microsoft

Carte réseau compatible NE2000

protocole NetBEUI

protocole compatible IPX/SPX

TCP/IP

Fichiers et imprimantes partagés pour les réseaux Microsoft

### Le partage de ressources

Il est très simple de partager et d'utiliser des ressources partagées sous Windows 9x, il suffit en effet de cliquer avec le bouton droit sur l'élément à partager (dossier, fichier, imprimante) et de choisir l'option *partager*. Si celle-ci n'apparaît pas, soit l'élément n'est pas "partageable", soit votre carte est mal installée auquel cas il faut recommencer les opérations ci-dessus...

Normalement vous devriez voir apparaître une fenêtre qui vous permet de donner un nom de partage et de mettre un mot de passe si vous voulez restreindre l'accès...

L'icône de la ressource partagée est alors agrémentée d'une main bleue...

Pour accéder aux ressources partagées, il vous suffit d'aller dans le voisinage réseau (un icône qui est apparu sur votre bureau) puis de vous "promener" d'un ordinateur à un autre... Pour utiliser une ressource partagée il vous suffit de double-cliquer sur celle-ci.

Dans le cas des imprimantes, il faut que les drivers de celle-ci soient présents sur les ordinateurs du réseau voulant l'utiliser. Pour cela le mieux est de cliquer avec le bouton droit sur la ressource (l'imprimante) dans le voisinage réseau, puis de choisir installer.

### Configurer le protocole TCP/IP

Les protocoles NetBEUI et IPX/SPX sont des protocoles simples qui n'ont pas besoin d'être configurés. Ces protocoles sont suffisants pour un réseau local, toutefois si vous reliez celui-ci à Internet ou si jamais celui-ci est grand, il vous faudra utiliser le protocole TCP/IP qui est le protocole utilisé sur Internet. Ce protocole utilise un système d'adresses uniques pour chaque ordinateur, appelées *adresses IP*, pour repérer un ordinateur sur le réseau. Ces adresses sont notées sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un nombre de 0 à 255 (ainsi l'adresse 192.56.32.255 est une adresse valide tandis que 126.256.2.3 est invalide).

Sur Internet, chaque ordinateur doit avoir sa propre adresse, il existe donc un organisme, l'INTERNIC, qui est chargé d'allouer des adresses IP aux ordinateurs qui sont connectés sur Internet.

Si votre réseau n'est pas connecté à Internet vous pouvez mettre les adresses IP que vous désirez aux ordinateurs du réseau local en faisant attention toutefois de mettre les mêmes trois premiers chiffres à tous (par exemple 125.2.3.6, 125.6.45.212 et 125.123.65.252).

Si votre réseau est connecté à Internet (c'est généralement pour cette raison que l'on installe le protocole TCP/IP sur un réseau local), il existe des adresses réservées par l'INTERNIC, c'est-à-dire des adresses que vous pouvez utiliser à loisir sur votre réseau local car elles ne seront pas prises en compte par les routeurs sur Internet et ne gêneront donc personne.

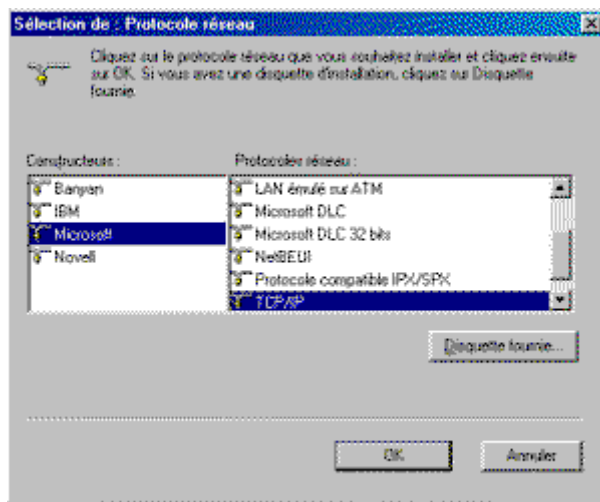
Il s'agit des adresses suivantes:

**10.0.0.0 à 10.255.255.255**

**172.16.0.0 à 172.31.255.255**

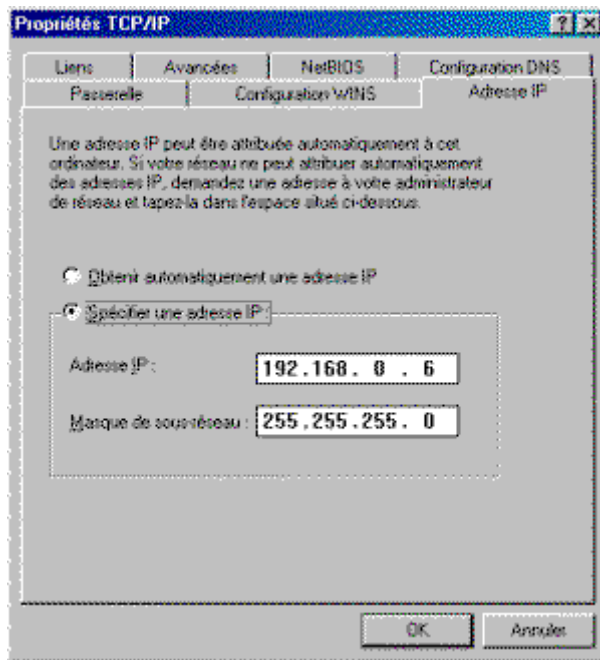
**192.168.0.1 à 192.168.255.255**

Pour installer le protocole TCP/IP allez dans *Panneau de configuration/Réseau/Ajouter/Protocole* puis choisissez TCP/IP sous le constructeur Microsoft Le CD de Windows vous sera probablement demandé)



Il vous faut maintenant spécifier une adresse IP unique pour chaque ordinateur du réseau local. Pour cela allez dans *Panneau de configuration/Réseau* et double-cliquez sur *TCP/IP*.

Dans l'onglet *Adresse IP* choisissez *spécifier une adresse IP* puis entrez pour chaque ordinateur une adresse IP faisant partie des adresses réservées ci-dessus (par exemple 192.168.0.1, 192.168.0.2, ...) Puis entrez 255.255.255.0 comme masque de sous-réseau pour tous les PC du réseau local.



Sur chaque machine du réseau créez un fichier texte appelé *lmhosts* (sans extension) dans le répertoire *c:\windows\* comprenant sur chaque ligne l'adresse IP puis le nom d'ordinateur associé, par exemple:

```
192.168.0.0      Master
192.168.0.1     Brochet
192.168.0.2     D@d
192.168.0.3     Flo
192.168.0.4     Jean
192.168.0.5     Ced
192.168.0.6     Romain
192.168.0.7     Mickey
192.168.0.8     Jeff
```

Cela permet d'associer les adresses IP à des noms pour plus de facilité...

Le réseau est maintenant prêt à fonctionner, il ne reste plus qu'à effectuer quelques tests pour vérifier son bon fonctionnement!

### Tester le protocole TCP/IP

Pour tester le bon fonctionnement d'un réseau il existe un utilitaire très pratique fourni en standard avec Windows, il s'agit de l'utilitaire **ping**, fonctionnant sous DOS, qui permet d'envoyer un paquet de donnée à un ordinateur du réseau et de regarder au bout de combien de temps il reçoit la réponse. Pour cela ouvrez une fenêtre "Commandes MS-DOS", puis effectuez successivement les étapes suivantes:

ping sur votre ordinateur grâce à l'adresse de boucle (127.0.0.1) qui représente votre ordinateur (**ping 127.0.0.1**)

ping sur chaque ordinateur du réseau (**ping 192.168.0.3** par exemple)

ping sur quelques noms d'ordinateur (**ping Mickey** par exemple)

Si tout cela fonctionne, votre réseau est apte à être utilisé!

## 12. L'avenir de la carte réseau - Conclusion

De notre avis, la carte réseau a encore une vie prometteuse. Ce qui va vraiment évoluer, c'est son débit (nous sommes déjà au Gigabits) et certainement le type de câble risque de changer (câble à fibre optique va se normaliser pour performer la vitesse). L'interface PCI risque de disparaître soit au profit d'une évolution (PCI-X) soit en intégrant la carte réseau sur la carte mère. On va voir aussi une évolution du sans fil (wifi) encore trop cher pour le moment pour être adopté par les particuliers. L'avenir de la communication entre les systèmes indépendant ne peut qu'évoluer.

- Exemples de cartes réseaux actuellement sur le marché :



**Carte PCMCIA :** Carte réseau PCMCIA WiFi 802.11g à 54 Mbps, TEW-421PC, TRENDnet, PC  
Prix : 29,95 €



**Carte PCI :** Carte réseau PCI WiFi 802.11g à 54 Mbps, TEW-423PI, TRENDnet, PC  
Prix : 31,95 €



**Carte FireWire :** Linksys Carte réseau PCMCIA sans fil WPC11-FR - 11 Mbit/s  
Prix : 28,00 €



**Carte réseau :** D-link Carte réseau D-LINK DFE-528TX - PCI - Fast Ethernet - 10/100Base-TX - 32  
Prix : 10,25 €



**Carte PCI :** Asus Carte réseau sans fil WiFi 802.11b, ASUS WiFi, point d'accès, Asus, PC  
Prix : 29,90 €



**Carte réseau :** Linksys Carte réseau externe USB 10/100 USB200M  
Prix : 27,00 €

## **Références :**

[http://www.leguide.net/free/go/search/nbtot/2142/id\\_rech/67832453/mot/carte\\_reseau/debut/0/go.htm](http://www.leguide.net/free/go/search/nbtot/2142/id_rech/67832453/mot/carte_reseau/debut/0/go.htm)  
<http://mir2003.free.fr/reseaux/cartesrezo.htm>  
<http://c.bravo.free.fr/ReseauxCHII.htm>  
<http://histoire.info.online.fr/net.html>  
<http://www.commentcamarche.net/pc/cartres.php3>  
<http://www.commentcamarche.net/transmission/transcabl.php3#connecteurspair>  
[http://perso.wanadoo.fr/arsene.perez-mas/reseaux/ieee802/802\\_3/csmacd.htm](http://perso.wanadoo.fr/arsene.perez-mas/reseaux/ieee802/802_3/csmacd.htm)  
<http://www.linux-france.org/prj/jargonf/T/transcepteur.html>  
<http://www.linux-france.org/prj/jargonf/P/plug-and-play.html>  
[http://perso.wanadoo.fr/arsene.perez-mas/reseaux/ieee802/802\\_3/802\\_3.htm](http://perso.wanadoo.fr/arsene.perez-mas/reseaux/ieee802/802_3/802_3.htm)  
<http://www.commentcamarche.net/elec/rj45croise.php3>  
<http://fr.tldp.org/HOWTO/lecture//Plug-and-Play-HOWTO.html>  
<http://www.haute-marne.cci.fr/fr/wifi/wifi.pdf>  
<http://0franc.free.fr/internet/histoire.htm>  
<http://www.dicofr.com/cgi-bin/n.pl/dicofr/definition/20010101002524>  
<http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/nic.html>  
<http://fr.wikipedia.org>  
<http://www.world-informatique.com/pasapas/reseaux/reseaux9.htm>  
<http://hautrive.free.fr/reseaux/supports/modes-de-transmission-des-signaux.html>



ERROR: syntaxerror  
OFFENDING COMMAND: --nostringval--

STACK:

(la carte reseau)  
/Title  
( )  
/Subject  
(D:20050103203935)  
/ModDate  
( )  
/Keywords  
(PDFCreator Version 0.8.0)  
/Creator  
(D:20050103203935)  
/CreationDate  
(Convert)  
/Author  
-mark-