

Module Réseaux Informatiques

Niveau : 04 Année ingénieur

Enseignant : BOUTINE RACHID

Plan du cours :

- ❖ Introduction
- Chronologie de développement des réseaux informatiques

Chapitre 1 : Principes des réseaux informatiques

- Classification des réseaux
- Moyens de transmission
- Notion de signal
- Le modèle en couches

Chapitre 2 : la couche physique

- Système de communication informatique
- Nature de circuit de données
- Synchronisation
- Codage en bande de base
- Codage en large bande.

Chapitre 3 : la couche liaison de données

- Définition d'une trame
- Protocole synchrones
- Protocoles COP
- Protocoles BOP
- Protocole asynchrones
- Les méthodes de détection d'erreurs
- Les méthodes de correction d'erreurs

Chapitre 4 : La couche réseau

- Définition d'un paquet
- Le contrôle de flux
- Le contrôle de congestion
- Le routage
- L'adressage

La méthode de progression durant ce cours est la suivante :

Le cours introduit des principes généraux et quelques exemples fondamentaux, les TDs font l'objet de séances particulières durant lesquelles les notions de cours sont rappelées, explicitées, et au besoin étendues, ils consistent en une série d'exercices d'application d'approfondissement, les TDs ainsi que leur correction sont évalués. des TPs seront énoncer selon le besoin.

Le but de ce cours est d'avoir une première idée, des moyens matériels et logiciels nécessaires pour qu'un ordinateur puisse communiquer avec un autre, ce cours comprend quatre parties:

La partie 1 traite les transmissions de données dans les réseaux en général sous l'angle de l'architecture des systèmes ouverts (modèle OSI). La partie 2 présente des notions concernant le réseau Internet et les protocoles qui lui sont associés. Les parties 3 et 4 sont plus orientées vers des applications pratiques visant la mise en place de services sur les réseaux. Ils sont plus particulièrement détaillés en TD et TP.

Les principales références bibliographiques en français sont :

- Initiation aux réseaux : cours et exercices 4394 – 4395 /08 ع!
- La transmission dans les réseaux informatiques : cours et exercices 4981 – 4975/08 ع!.
- Les Protocoles dans les réseaux informatiques : cours et exercices 4229 – 4227 /08 ع!.

*/*Pour illustrer une idée d'une façon claire , il faut poser la question et ensuite répondre aux 5 questions fondamentaux quoi , où, quand, par qui, comment?*/*

Introduction

Les premiers réseaux ne sont pas informatiques mais liés aux télécommunications. Les réseaux du télégraphe (à partir de 1850) puis du téléphone, puis du télétype sont les ancêtres des réseaux informatiques d'aujourd'hui . Par exemple, le système de codage Morse est à la base des techniques de numérisation¹ actuelles. Le symbole **A** par exemple, est codé en Morse par « *trait court, trait long* | | » pour être transmis par le télégraphe. Aujourd'hui on peut dire que le principe reste le même mais c'est le code qui a changé : ce sera peut être son code ASCII (**01000001**) qui sera transmis sur les câbles électriques. Au niveau physique, les réseaux fonctionnent alors selon des règles similaires, un échange d'impulsions électriques sur un fil, plus ou moins longues pour le Morse, ou alternées pour les réseaux modernes. Lorsque sur le support de communication les informations à transmettre sont codées en binaire, on parle de réseau numérique.

Le réseau téléphonique est régi par un principe différent. La voix est convertie par le microphone (une membrane qui bouge en fonction du mouvement d'air que forme le son) en signal électrique qui varie en hauteur et fréquence (c'est une modulation) selon le volume et la hauteur du son à transmettre. De l'autre côté, le signal électrique est transformé par le haut parleur (une nouvelle membrane qui fait l'opération inverse). C'est le principe du fameux téléphone des enfants construit avec une cordelette et deux pots de yaourt. On parle alors de réseau analogique en opposition aux réseaux numériques.

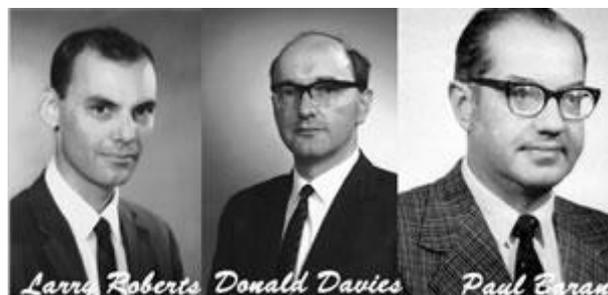
Les années 60 : contexte de la guerre froide

En 1957, suite au lancement du premier satellite Spoutnik par les Soviétiques, le président 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 ennemis Russes. Cette organisation regroupait certains des plus brillants cerveaux américains qui développèrent le premier satellite opérationnel des US en 18 mois. Quelques années après, l'ARPA commença à s'intéresser aux réseaux d'ordinateurs et aux technologies de la communication.

En 1967, Lawrence G. Roberts, récemment arrivé à la tête du projet de réseau informatique à l'ARPA, publie ses "Plans pour le réseau ARPANET" . il a aussi publié un papier sur un concept de réseau à commutation de paquets.

Les militaires s'inquiétaient en effet de voir les dirigeants des USA privés de communication si les lignes de téléphones disparaissaient après un bombardement. Ainsi ils s'intéressaient à l'idée des paquets passant de noeud en noeud ayant la même autorité sans système central, une anarchie technologique qui même en cas de destruction partielle du réseau, en cas de guerre nucléaire pourrait continuer à fonctionner.

C'est ainsi que l'histoire de l'internet a commencé.



Chronologie de développement des réseaux et des télécommunications

1940 : première communication à distance entre machines à calculer

Le 11 septembre 1940, George Stibitz de Bell Labs communique par téléscripteur à partir du Dartmouth College, New Hampshire, et fait fonctionner à distance, une machine à calculer à relais située à New York.

1957 : lancement du projet ARPA

Le lancement du satellite Sputnik par l'URSS amène les Américains à créer à l'intérieur de son Département de la défense une agence nommée ARPA (*Advanced Research Projects Agency*) dont le but est d'établir une avance américaine dans le domaine de la science et de la technologie à des fins militaires.

1960 : le premier réseau d'ordinateurs

C'est en 1960, qu'on a installé le premier véritable réseau d'ordinateurs, dans le cadre du système de surveillance aérienne SAGE (*Semi-Automatic Ground Environment*). Des dizaines de radars postés aux frontières stratégiques se partageaient le soin de constituer en temps réel, une carte complète du ciel qui était centralisée grâce à quarante ordinateurs géants reliés par des lignes téléphoniques (Breton et Proulx, 1989).

1962 : premier réseau commercial

En 1962, American Airlines est la première entreprise commerciale au monde à se doter d'un système de réservation de billets d'avion par ordinateur. C'est le premier grand réseau commercial d'ordinateurs, le *SABRE*, installé par IBM.

1969 : ARPAnet, premier réseau informatique pour la recherche

ARPAnet (*Advanced Research Projects Agency network*) est, à l'origine, un réseau conçu par le Département américain de la défense pour étudier le fonctionnement des réseaux d'ordinateurs et pour permettre à des chercheurs de s'échanger de l'information. La communication sur le réseau se fait par paires d'ordinateurs possédant chacune une adresse, qui s'échangent des informations selon un protocole appelé *Internet Protocol* (IP). Sur le réseau, n'importe lequel ordinateur est capable de communiquer avec n'importe quel autre. De plus, *ARPAnet* permet de réorienter la communication sur un autre nœud du réseau, en cas de coupure de la communication. Cette façon de faire permet de garder fonctionnel le réseau même si l'un des nœuds tombe en panne.

1971 : invention d'un logiciel de courrier électronique

Ray Tomlinson de BBN crée un logiciel pour envoyer des messages à l'intérieur d'un réseau distribué.

1973 : première connections internationales à l'ARPANET

L'University College of London d'Angleterre et le Royal Radar Establishment de Norvège se branche à ARPANET.

1978 : le Vidéotex

Le vidéotex (ou vidéographie) est une technologie qui permet de transmettre de l'information textuelle ou graphique stockée dans un ordinateur, sur des écrans de télévision, que ce soit sous forme interactive (Videotex) ou non interactive (Télétexte). Les Anglais et les Français ont été les premiers à expérimenter cette technologie dans leur projet *Prestel* et *Minitel*, avec les succès que l'on connaît aujourd'hui

1980 : INTERNET

Au début des années 1980, prolifère dans les universités américaines, toute une génération de postes de travail individuel qui viennent remplacer les gros ordinateurs à temps partagés. Ces postes de travail tournent sous *UNIX* et permettent la communication en réseau. Désormais, ce ne sont plus seulement quelques grosses machines qui sont branchées sur le réseau *ARPAnet* mais de nombreuses petites machines individuelles. En 1991, le Congrès américain vote un budget de 400 millions de dollars pour relier des chercheurs entre eux et permettre aux écoles américaines de la maternelle jusqu'à la fin du *high school* d'être reliées au réseau Internet. On décide également d'ouvrir Internet au commerce. L'idée est lancée de créer l'autoroute de l'information. C'est ainsi qu'Internet connaît une expansion formidable non seulement aux états-unis mais également partout dans le monde.

1990 : naissance du World Wide Web (WWW)

Au début de 1990, le Centre d'étude et de recherche nucléaires, le CERN, dont le siège est situé à Genève en Suisse, lance le *World Wide Web* (WWW) pour permettre aux chercheurs d'échanger rapidement des informations textuelles y compris des images fixes ou animées et du son. Cette nouvelle façon d'échanger de l'information deviendra très vite populaire grâce aux logiciels de navigation hypertextuelle qui en facilitent l'accès. Le premier de ceux-ci, *Mosaic*, a été mis au point au *National Center for Supercomputing Applications* (NCSA) à University of Illinois, par un groupe d'étudiants.

1994 : explosion de Internet avec le World Wide Web (WWW)

L'année 1994 est l'année de Internet qui connaît une expansion fulgurante avec l'arrivée massive des entreprises sur le World Wide Web qu'on accède grâce à des interfaces graphiques comme Internet explorer, *Mosaic* ou *Netscape*.

Chapitre 1 : Principe des réseaux numériques.

Dans ce chapitre nous aborderons les grands principes régissant les équipements matériels et logiciels permettant d'échanger des données mises sous forme numérique et qui forment les réseaux informatiques.

I-1 Définitions :

- **Réseau** : C'est un ensemble d'ordinateurs (ou de périphériques) autonomes connectés entre eux et qui sont situés dans un certain domaine géographique.
- **Téléinformatique** = informatique à distance. C'est une science qui associe les problèmes liés au traitement des données et aux problèmes liés au transport de l'information.

I - 2. Qu'apportent les réseaux

Les Réseaux permettent :

- De partager les fichiers.
- Le transfert de fichier.
- Le partage d'application : compilateur, système de gestion de base de donnée (SGBD).
- Partage d'imprimante.
- L'interaction avec les utilisateurs connectés : messagerie électronique, conférence électronique, Talk, ...
- Le transfert de donnée en générale (réseaux informatiques).
- Le transfert de la parole (réseaux téléphoniques).
- Le transfert de la parole, de la vidéo et des données (réseaux à intégration de services ou multimédia).

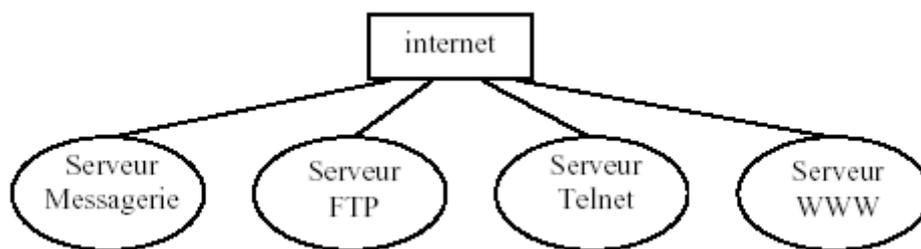
I - 3. Vocabulaire de base

Station de travail : on appelle station de travail toute machine capable d'envoyer des données vers les réseaux (PC, MAC, SUN Terminale X, ...). Chaque station de travail à sa propre carte interface (carte réseau).

Nœud : c'est une station de travail, une imprimante, un serveur ou toute entité pouvant être adressée par un numéro unique.

L'unicité de l'adresse est garantie par le constructeur d'une carte réseau qui donne un numéro unique ne pouvant être changé par personne.

Serveur : dépositaire centrale d'une fonction spécifique : serveur de base de donnée, de calcul, de fichier,....



Paquet : C'est la plus petite unité d'information pouvant être envoyée sur le réseau. Un paquet contient en général l'adresse de l'émetteur, l'adresse du récepteur et les données à transmettre.

Topologie : organisation physique et logique d'un réseau. L'organisation physique concerne la façon dont les machines sont connectées (Bus, Anneau, Étoile, Maillé, Arborescence, ...). La topologie logique montre comment les informations circulent sur le réseau (diffusion, point à point).

I-4 Classification des réseaux :

Les réseaux informatiques qui permettaient à leur origine de relier des terminaux passifs à des gros ordinateurs centraux autorisent à l'heure actuelle l'interconnexion de tous types, d'ordinateurs que ce soit de gros serveurs, des stations de travail, des ordinateurs personnels ou de simples terminaux graphiques. Les services qu'ils offrent font partie de la vie courante des entreprises et administrations (banques, gestion,

commerce, bases de données, recherche, etc...) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet ...).

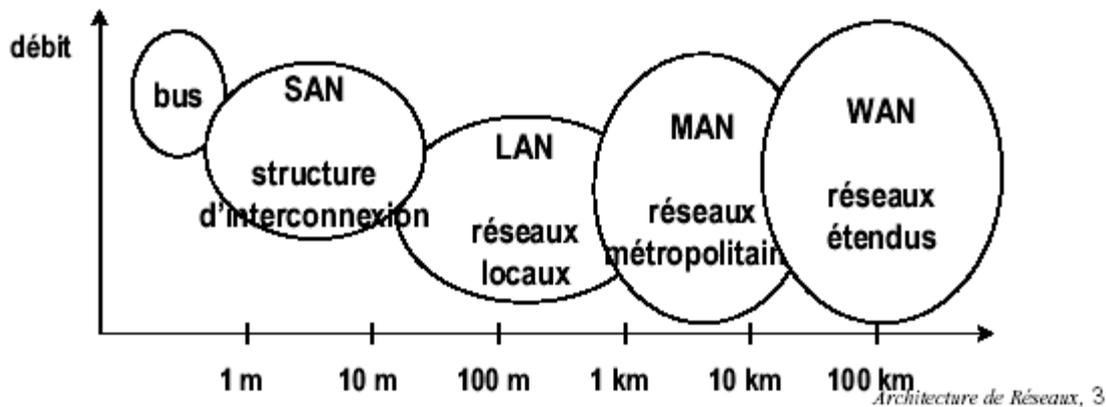


Figure 1.1 : Selon la distance qui sépare les ordinateurs

I-4-1 Selon la taille du réseau

On peut faire une première classification des réseaux à l'aide de leur taille comme on peut le voir dans la figure 1.1.

- **Les bus** que l'on trouve dans un ordinateur pour relier ses différents composants (mémoires, périphériques d'entrée-sortie, processeurs, ...) peuvent être considérés comme des réseaux dédiés à des tâches très spécifiques.
- **Les structures d'interconnexion** sont des réseaux de très haut débit, mais de faible étendue, et regroupent les pré et post-processeurs des ordinateurs vectoriels par exemple. En effet l'usage d'un super-calculateur (Cray notamment) nécessite un ordinateur, dit frontal, qui lui prépare les données et recueille les résultats. (Structure Area Network)
- **Un réseau local** (Local Area Network) peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.
- **Un réseau métropolitain** (Metropolitan Area Network) interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.
- **Un réseau étendu** (Wide Area Network) permet de communiquer à l'échelle d'un pays, ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.

I-4-2 Selon la topologie

Figure 1.2 : Selon la topologie des réseaux

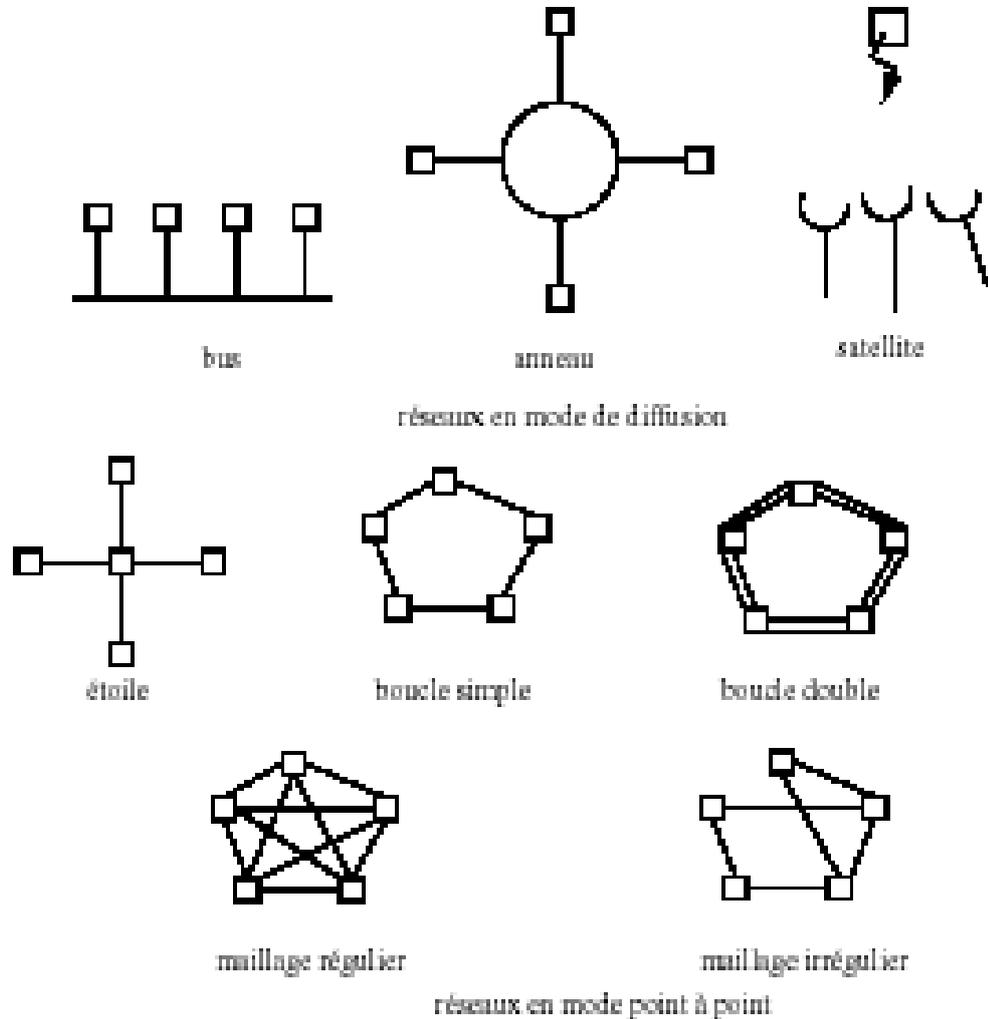


FIG. 1.2 - Topologie des réseaux informatiques.

I-4-3 Selon le mode diffusion

On peut également différencier les réseaux selon leur mode diffusion :

- ceux en mode de diffusion
- ceux en mode point à point

Le mode en diffusion :

Ce mode de fonctionnement consiste à partager un seul support de transmission. Chaque message envoyé par un équipement sur le réseau est reçu par tous les autres. C'est l'adresse spécifique placée dans le message qui permettra à chaque équipement de déterminer si le message lui est adressé ou non. À tout moment un seul équipement a le droit d'envoyer un message sur le support, il faut donc qu'il écoute au préalable si la voie est

libre; si ce n'est pas le cas il attend selon un protocole spécifique à chaque architecture. Les réseaux locaux adoptent pour la plupart le mode diffusion sur une architecture en bus ou en anneau et les réseaux satellitaires ou radio suivent également ce mode de communication. Dans une telle configuration la rupture du support provoque l'arrêt du réseau, par contre la panne d'un des éléments ne provoque pas (en général) la panne globale du réseau.

Le mode point à point :

Dans le mode diffusion point à point le support physique (le câble) relie une paire d'équipements seulement. Quand deux éléments non directement connectés entre eux veulent communiquer ils le font par l'intermédiaire des autres nœuds du réseau.

Dans le cas de l'étoile le site central reçoit et envoie tous les messages, le fonctionnement est simple, mais la panne du nœud central paralyse tout le réseau

Dans une boucle simple, chaque nœud recevant un message de son voisin en amont le réexpédie à son voisin en aval. Pour que les messages ne tournent pas indéfiniment le nœud émetteur retire le message lorsqu'il lui revient.

Si l'un des éléments du réseau tombe en panne, alors tout s'arrête. Ce problème est partiellement résolu par la double boucle dont chacune des boucles fait tourner les messages dans un sens opposé. En cas de panne d'un équipement, on reconstitue une boucle simple avec les éléments actifs des deux boucles, mais dans ce cas tout message passera deux fois par chaque nœud. Il en résulte alors une gestion plus complexe.

Dans le maillage régulier l'interconnexion est totale ce qui assure une fiabilité optimale du réseau, par contre c'est une solution coûteuse en câblage physique. Si l'on allège le plan de câblage, le maillage devient irrégulier et la fiabilité peut rester élevée mais elle nécessite un routage des messages selon des algorithmes parfois complexes. Dans cette architecture il devient presque impossible de prévoir le temps de transfert d'un nœud à un autre.

I-4-4 Selon le mode de connexion :

Quelle que soit l'architecture physique d'un réseau on trouve deux modes de fonctionnement différents :

- avec connexion
- sans connexion

Le mode avec connexion :

Dans ce mode toute communication entre deux équipements suit le processus suivant:

1. l'émetteur demande l'établissement d'une connexion par l'envoi d'un bloc de données spécial.
2. si le récepteur (ou le gestionnaire de service) refuse cette connexion la communication n'a pas lieu.
3. si la connexion est acceptée, elle est établie par mise en place d'un circuit virtuel dans le réseau reliant l'émetteur au récepteur
4. les données sont ensuite transférées d'un point à l'autre.
5. la connexion est libérée

C'est le fonctionnement bien connu du réseau téléphonique classique. Les avantages du mode avec connexion sont la sécurisation du transport par identification claire de l'émetteur et du récepteur, la possibilité d'établir à l'avance des paramètres de qualité de service qui seront respectés lors de l'échange des données. Les défauts sont la lourdeur de la mise en place de la connexion qui peut se révéler beaucoup trop onéreuse si l'on ne veut échanger que quelques octets ainsi que la difficulté à établir des communications multipoint.

Le mode sans connexion :

Dans le mode sans connexion les blocs de données, appelés datagrammes, sont émis sans vérifier à l'avance si l'équipement à atteindre, ainsi que les nœuds intermédiaires éventuels, sont bien actifs.

C'est alors aux équipements gérant le réseau d'acheminer le message étape par étape et en assurant éventuellement sa temporisation jusqu'à ce que le destinataire soit actif. Ce service est celui du courrier postal classique et suit les principes généraux suivants:

- le client poste une lettre dans une boîte aux lettres.
- chaque lettre porte le nom et l'adresse du destinataire.
- chaque client a une adresse propre et une boîte aux lettres.
- le contenu de l'information reste inconnu du prestataire de service.

- les supports du transport sont inconnus de l'utilisateur du service.

I-4-5 Selon le mode de commutation :

Le réseau doit permettre l'échange de messages entre les abonnés quelle que soit leur localisation.

Définition : La commutation rassemble toutes les techniques qui réalise la mise en relation de 2 abonnés quelconques. Il existe 4 techniques de commutation :

- **la commutation de circuits** : c'est historiquement la première à avoir été utilisée, par exemple dans le réseau téléphonique à l'aide des auto-commutateurs. Elle consiste à créer dans le réseau un circuit particulier entre l'émetteur et le récepteur avant que ceux-ci ne commencent à échanger des informations. Ce circuit sera propre aux deux entités communicantes et il sera libéré lorsque l'un des deux coupera sa communication. Par contre, si pendant un certain temps les deux entités ne s'échangent rien le circuit leur reste quand même attribué. C'est pourquoi, un même circuit (ou portion de circuit) pourra être attribué à plusieurs communications en même temps. Cela améliore le fonctionnement global du réseau mais pose des problèmes de gestion (files d'attente, mémorisation,...etc).
- **la commutation de messages** : elle consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de noeud de commutation en noeud de commutation. Chaque noeud attend d'avoir reçu complètement le message avant de le réexpédier au noeud suivant. Cette technique nécessite de prévoir de grandes zones tampon dans chaque noeud du réseau, mais comme ces zones ne sont pas illimitées il faut aussi prévoir un contrôle de flux des messages pour éviter la saturation du réseau. Dans cette approche il devient très difficile de transmettre de longs messages.
- **la commutation de paquets** : elle est apparue au début des années 70 pour résoudre les problèmes d'erreur de la commutation de messages. Un message émis est découpé en paquets et par la suite chaque paquet est commuté à travers le réseau comme dans le cas des messages. Les paquets sont envoyés indépendamment les uns des autres et sur une même liaison on pourra trouver les uns derrière les autres des paquets appartenant à différents messages. Chaque noeud redirige chaque paquet vers la bonne liaison grâce à une table de routage. La reprise sur erreur est donc ici plus simple que dans la commutation de messages, par contre le récepteur final doit être capable de reconstituer le message émis en réassemblant les paquets. Ceci nécessitera un protocole particulier car les paquets peuvent ne pas arriver dans l'ordre initial, soit parce qu'ils ont emprunté des routes différentes, soit parce que l'un d'eux a du être réémis suite à une erreur de transmission.
- **la commutation de cellules** : une cellule est un paquet particulier dont la taille est toujours fixée à 53 octets (5 octets d'en-tête et 48 octets de données). C'est la technique de base des réseaux hauts débits ATM (Asynchronous Transfert Mode) qui opèrent en mode connecté où avant toute émission de cellules, un chemin virtuel est établi par lequel passeront toutes les cellules. Cette technique mixe donc la commutation de circuits et la commutation de paquets de taille fixe permettant ainsi de simplifier le travail des commutateurs pour atteindre des débits plus élevés.

II-1 – Moyens de transmission

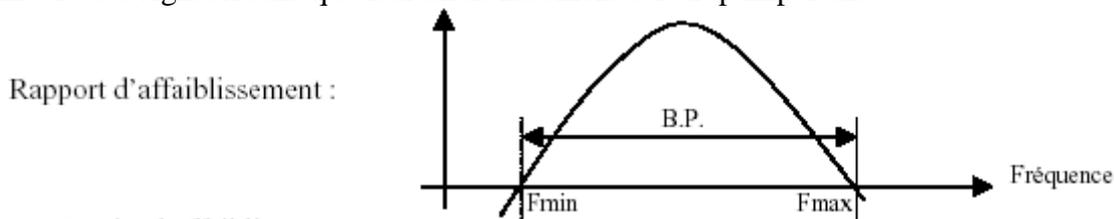
II-1-1 Les principaux supports utilisés : métalliques, ondes, fibres optiques.

- **Support métallique** : reposent sur la propriété de conductivité électrique des métaux (cuivre, bronze, ...).
 - **Paire de fils torsadés**.
 - **Câble coaxial** : – câble fin (Ethernet fin) – gros câble (gros Ethernet).
- **Fibre optique** : la transmission se fait par propagation d'un rayon lumineux dans une fibre de verre.
- **Hertzienne** : Utilise des ondes radio – électriques. La propagation se fait par ligne droite (radio, télé, ...) pour permettre des liaisons grandes distance, on utilise des satellites.
 - **Avantages** : liaison grande distance. Pas de câblage.
 - **Inconvénients** : affaiblissement des signaux et le temps de propagation est de 260 ms pour un aller – retour.

11-1-2 caractéristiques des supports de transmission

Les caractéristiques des supports de transmission (débit, taux d'erreurs) dépendent de la bande passante, et de l'affaiblissement du signal ... etc, et de la façon d'utiliser le support pour transmettre des données (multiplexage ou non, ...).

Bande Passante : La bande passante d'une voie est la plage de fréquence sur laquelle la voie est capable de transmettre des signaux sans que leur affaiblissement soit trop important.



Courbe d'affaiblissement : Valeur du rapport d'affaiblissement en fonction de la fréquence.

Le rapport d'affaiblissement = (Amplitude du signal émis / Amplitude du signal reçu)

Capacité d'une voie : Quantité d'information pouvant être transmise en une seconde. S'exprime en bit/s.

Voir aussi la notion de bauds, liées à la valence.

Longueur élémentaire d'une voie : Longueur (en mètres) au-delà de laquelle le signal doit être amplifié ou répété pour être correctement reçu.

La longueur élémentaire est plus important dans le cas de la fibre optique que dans le cas du coaxial.

Temps de transfert :

Durée qui sépare le début d'émission de la fin de réception : $T_{\text{transfert}} = T_{\text{émission}} + T_{\text{propagation}}$.

Taux d'erreur : Probabilité de perte ou d'altération d'une information (1 bit). On peut la mesurer en calculant pendant un temps significatif le rapport du nombre de bits erronés sur le nombre de bits émis.

II-2 – Notion de signal

Pour transmettre des informations binaires sur un support physique de transmission, il est nécessaire de les transformer au préalable en un signal électrique. Le signal électrique peut prendre la forme d'une suite d'impulsions obtenues par une correspondance directe entre les impulsions les représentant

Figure: Signal carré de la séquence de bits 1010.



Les supports de transmission usuels atténuent, déforment et retardent les signaux électriques. Ces supports de

transmission sont en plus sensibles a des perturbations d'origine interne au support lui même , mais également a des perturbations induites par l'environnement externe.

Certains supports , tels que les lignes utilisées par le réseau téléphonique commuté, sont mal adaptées à la transmission des signaux rectangulaires, car conçus au départ pour la transmission des signaux analogiques de fréquence limitée .

Ces défauts se manifestent généralement comme une adjonction, la suppression, ou l'inversion d'un ou de plusieurs bits. Le taux d'erreurs est en fonction du support utilisé et du signal véhiculant les informations

II-2-2 Caractéristiques des supports de transmission :

un support physique de transmission peut être de nature très diverse : paire de fils métalliques, câble coaxial, fibre optique, atmosphère ...etc , il est caractérisé par les effets indésirables qu'il exerce sur les signaux qui le traversent . certains de ces effets sont dus a la nature même du support de transmission d'autres sont dus à l'environnement externe.

II-2-2 -1 Atténuation et retardement:

Un canal réel atténue (affaiblit) l'amplitude du signal qui le traverse. Le phénomène d'atténuation est du à une perte d'énergie au sein du canal et s'accroît avec la longueur de celui-ci. Le phénomène d'atténuation peut être compensé par des amplificateurs.

On mesure l'atténuation par le rapport A_s/A_e ou A_s est l'amplitude du signal à la sortie du canal et A_e est l'amplitude du signal à l'entrée du canal. En général en mesure ce rapport en décibels sous la forme $20\log_{10}(A_s/A_e)$. Exemple $A_s/A_e=1/10 \rightarrow$ l'atténuation = -20db

En plus de l'atténuation un canal réel retarde les signaux qui le traversent.

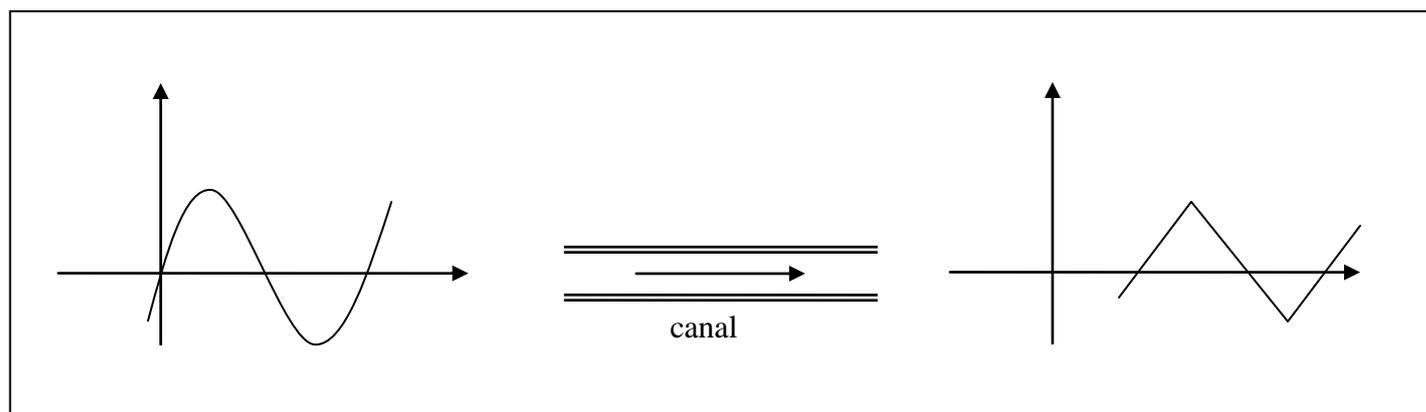
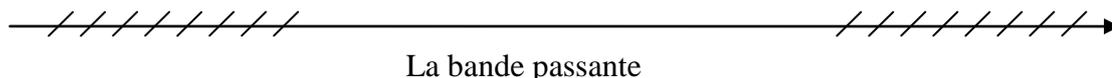


Figure N° : illustration des phénomènes d'atténuation et de retardement subis par un signal sigmoïdal traversant un canal réel

II-2-2 -2 Le filtrage :

Un canal réel se comporte généralement comme un filtre qui ne laisse donc passer qu'une bande limitée de fréquences. Toute fréquence en dehors de cette bande est tout simplement éliminée



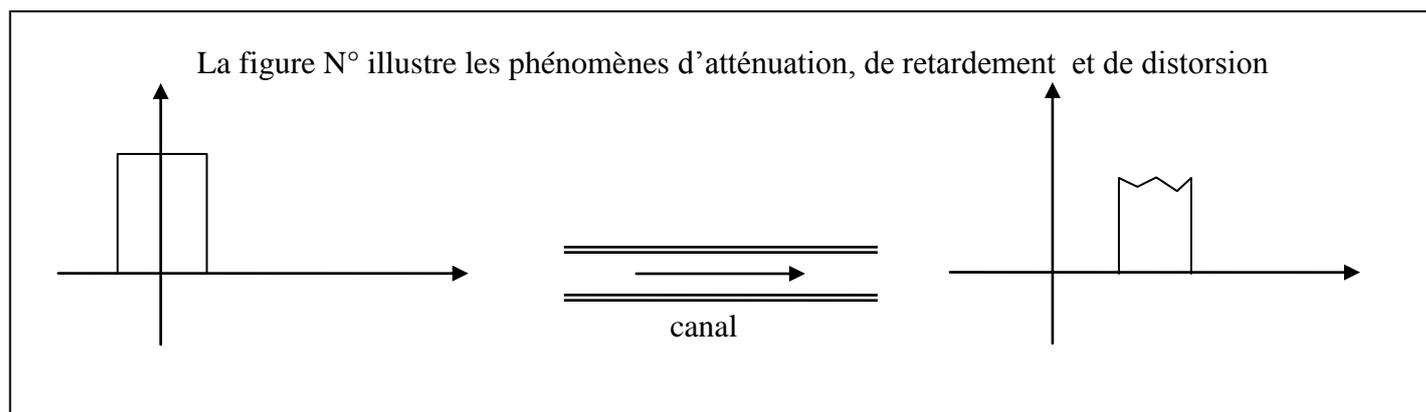
La figure N° : illustration de la bande passante d'un support de transmission

II-2-2 -3 la distorsion :

Un canal réel ne se comporte pas comme un filtre idéal et les fréquences qu'il laisse passer ne sont pas toutes atténuées et retardées dans les mêmes proportions.

En d'autres termes l'atténuation et le retardement sont fonction de la fréquence. Le résultat en est que le signal a la sortie du canal se trouve déformé. La figure ci-dessous illustre l'effet combiné des phénomènes

d'atténuation, de retardement et de distorsion auquel est soumis un signal rectangulaire lorsqu'il traverse un canal réel.



l'effet du phénomène de distorsion peut être compensé par des dispositifs nommés égaliseurs (equalisers). Ces dispositifs sont placés au niveau de l'émetteur ou au niveau du récepteur.

II-2-2-4 le bruit :

Le bruit est un signal perturbateur provenant du canal lui-même ou de son environnement externe. Il est de comportement aléatoire et vient s'ajouter au signal véhiculant les informations et provoquer ainsi des erreurs de transmission. On distingue généralement deux types de bruit le bruit blanc et le bruit impulsif.

1 le bruit blanc

Le bruit blanc est provoqué par une agitation thermique due essentiellement au mouvement des électrons et à la recombinaison des transporteurs au sein des semi-conducteurs. Ce type de bruit est uniformément repart sur toute la bande passante du canal.

2 le bruit impulsif

Ce phénomène est à caractère impulsif, les impulsions ont une valeur très élevée et une durée très brève. Il est de cause externe par exemple voisinage d'autres canaux, des bobines électro-magnétique, le vent solaire... etc.

Il est souvent possible de protéger ces canaux du bruit impulsif, mais il est impossible de les protéger contre le bruit blanc.

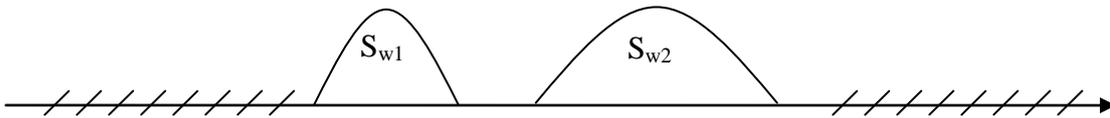
En évalue l'importance intensité du bruit en calculant le rapport S/B (S : l'amplitude du signal véhiculant l'information et B l'amplitude du bruit) est généralement exprimée en décibel comme suit : $20 \log_{10}(S/B)$. cette valeur se décroît avec la distance parce que le signal s'affaiblit et le bruit reste constant ce qui rend très limité le rôle des amplificateurs parce que en amplifiant le signal S c'est le bruit B aussi que se trouve amplifié

II-2-3 l'interférence:

Nous savons d'après le théorème de Fourier qu'un signal rectangulaire se compose d'un nombre infini de fréquences. Un canal réel, caractérisé par une bande passante limitée ne peut donc en aucun cas transmettre fidèlement un tel signal et celui-ci ne peut être transmis qu'amputé de ses fréquences se trouvant en dehors de la bande passante du canal.

Cependant pour garantir une transmission correcte du signal, il n'est pas nécessaire que le canal transmette fidèlement toutes les fréquences du signal mais seulement la largeur de bande du signal. Définie comme étant l'ensemble des fréquences où est localisé l'essentiel de l'énergie du signal.

Lorsque la bande passante d'un canal est suffisamment large, il est plus intéressant de la partager entre plusieurs signaux sans chevauchement.



La figure N° : illustration de la bande passante d'un support de transmission

11.2.4 Exemple de l'ADSL

La technique de l'ADSL (**Asymmetric bit rate Digital Subscriber Line** ou **ligne numérique d'abonnés à débits asymétriques**) est une technique récente qui permet d'utiliser, sur de courtes distances, les lignes téléphoniques classiques mais avec un débit très supérieur à celui des normes plus classiques (V34 ou V90). Par exemple, dans sa version Lite, elle permet de connecter à Internet un particulier en utilisant simplement sa ligne téléphonique habituelle comme illustré dans la figure 1.12.

De manière théorique, cette technologie offre un débit maximal descendant (d'Internet vers l'abonné) de 8,2 M bit/sec et un débit maximal montant (de l'abonné vers Internet) de 640 K bit/sec. Cependant, ces performances ne sont pas possibles sur une grande distance (plus de 5 km) et les solutions commerciales grand public proposées actuellement fixent par exemple le débit entrant à 512 Kbit/sec et le débit sortant à 128 Kbit/sec.

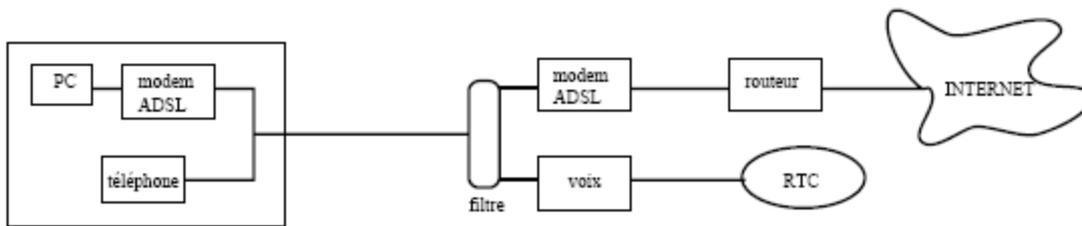


FIG. 1.12 - Connexion à Internet via ADSL Lite.

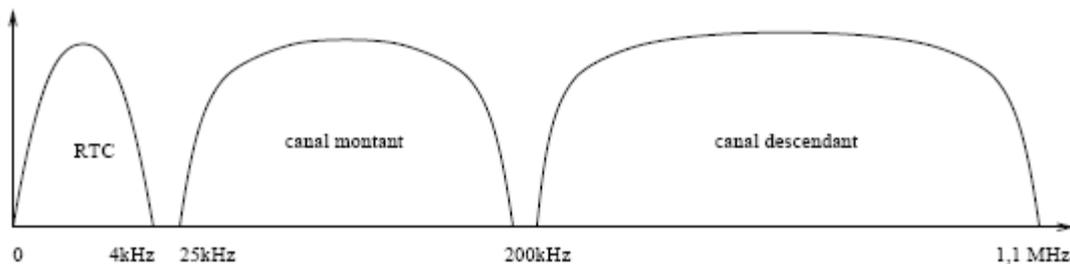


FIG. 1.13 - Multiplexage fréquentiel utilisé par ADSL (échelle des fréquences non réelles).

D'un point de vue technique ADSL fonctionne en full duplex grâce à un multiplexage fréquentiel, permettant de faire transiter simultanément les signaux montant et descendant accompagnés également des signaux portant la voix téléphonique. La figure 1.13 illustre ce multiplexage dans le cas où les fréquences pour les voies montantes et descendantes ont été clairement séparées. Pour gagner encore en largeur de bande, et donc en débit, on peut envisager de rapprocher les deux espaces de fréquences mais il faut alors annuler les perturbations (phénomène d'écho) que subissent les signaux montant et descendant émis simultanément.

Les différents signaux sont transmis selon la technologie DMT (Discrete MultiTone) qui divise la totalité de la bande passante en 256 sous-canaux d'une largeur de 4,3 kHz. Ainsi, le 1er canal est réservé à la téléphonie. Les canaux 2 à 6 servent à séparer la voix des données numériques. Le flux montant occupe les 32 canaux suivants et le flux descendant tous les canaux restant, dans le cas où aucune zone de fréquence ne sépare les deux sens de communication et que l'annulation d'écho est en place. Le fait que la largeur de bande montante soit plus faible que la descendante explique le terme asymétrique dans la dénomination ADSL. De plus, certains sous-canaux sont utilisés pour la gestion de la transmission

Chacun des sous-canaux est modulé indépendamment en utilisant la technique du QAM (Quadrature amplitude modulation), qui est une méthode de modulation d'amplitude de deux porteuses en quadrature (4 niveaux d'amplitude). Avant tout transfert de données, une procédure de négociation (handshake) est mise en place pour mesurer la qualité de la transmission et l'adapter en fonction de la ligne. On appelle cette technique rate adaptative, car elle est capable de diminuer le débit si la qualité de la transmission se dégrade.

II-3 – Architecture des réseaux

Au début des années 70, chaque constructeur a développé sa propre solution réseau autour d'architecture et de protocoles privés (SNA d'IBM, DECnet de DEC, DSA de Bull, TCP/IP du DoD,...) et il s'est vite avéré qu'il serait impossible d'interconnecter ces différents réseaux hétérogènes si une norme internationale n'était pas établie.

Alors, une normalisation de l'architecture logicielle s'impose. Deux grandes familles d'architectures se disputent le marché. La première provient de l'ISO et s'appelle OSI (Open System Interconnection).

La deuxième est TCP / IP. Une 3ème Architecture plus récente est UIT - T (Union Internationale des Télécommunications). Il s'agit de l'adaptation du modèle OSI pour prendre en compte les réseaux haut - débit (réseau ATM).

modèle de référence OSI

L'ISO a défini une architecture logicielle formée de 7 couches.

Intérêt : Bien séparer les problèmes.

Fonctionnement : Chaque couche (n) offre un certain nombre de services à la couche (n+1) en déroulant un protocole uniquement défini à partir des services fournis par la couche (n-1).

Structure en couches : *modèle OSI à 7 couches*

Le concept de l'OSI nécessite la compréhension de 3 concepts.

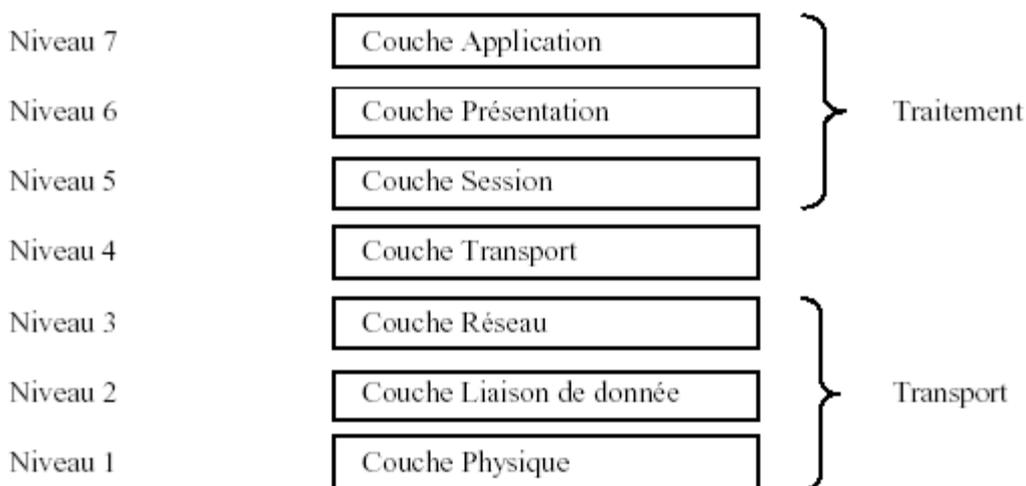
1. Le service (N)
2. Le protocole (N)
3. Le point d'accès à un service (N-SAP)
 - **Service (N)** : Ensemble d'événements et primitives pour rendre au niveau (n+1)
 - **Protocole (N)** : Ensemble de règles nécessaires pour le service (N) soit réalisé
 - **N-SAP** : Point situé à la frontière entre les couches (n) et (n+1).

L'architecture OSI est schématisée comme suit :

Un protocole est un ensemble de règles de communication et de messages assurant un service de communication.

- Protocole propriétaire : Pour chaque marque d'ordinateur correspond un protocole différent. Problèmes de compatibilité. Nécessité d'utiliser des interfaces...

- Protocole ouvert : Le concept OSI (Open System Interconnection) de l'ISO (International Standard Organisation). Toutes communications passent par un seul réseau ouvert, qui assure le transfert des informations, ce qui rend tout le monde compatible.



Couche physique : Assure le transfert de bit. Ce niveau rassemble les propriétés qui spécifient les caractéristiques mécaniques, électriques et fonctionnelles des circuits de données.

On trouve dans cette couche :

- L'étude des interfaces de connexion (fonction) : interface analogique V24 et numérique X21.
- L'étude des modems
- Les multiplexeurs et concentrateurs
- Les nœuds de commutation.

Couche liaison de données : Connexion entre entité, Correction des erreurs, partage du support Responsable de l'acheminement d'unités de données appelées trames en assurant la meilleure qualité de transmission possible. Une trame est une suite structurée de bits. Protocole standard : HDLC (High Data Level Link Control).

Couche réseau : • Connexion sur système ouvert (passerelles, ...), Adressage, Routage, Contrôle de Flux Offre un nombre de services dont un service d'adressage (IP) permettant d'atteindre son destinataire, un service de routages déterminant un chemin à l'intérieur du réseau maillé et un contrôle du flux pour ne pas saturer le réseau.

Transporte des unités de données de taille fixe appelée paquets. Exemple de protocole standards : X25 et IP.

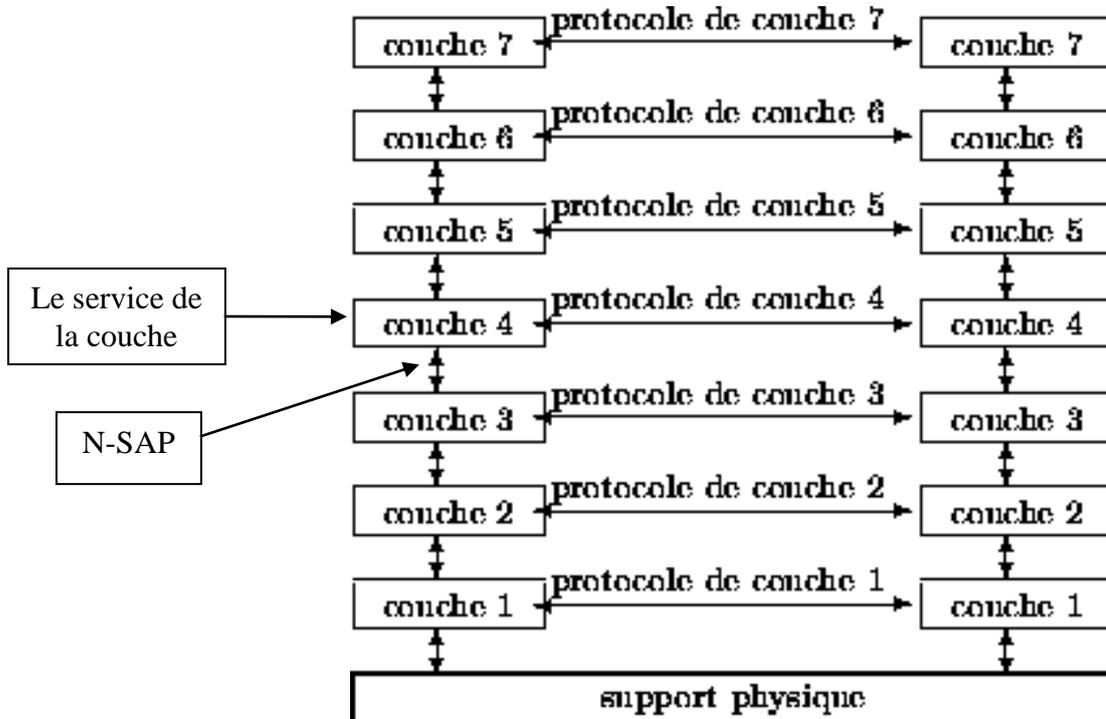
Couche transport : Optimise l'utilisation de la couche réseau et assure des travaux de type fragmentation de message (ex. TCP). Qualité de Service, Assemblage, Reprise sur Perte de Message, Contrôle de Flux Transporte des unités de données appelées messages. Protocole TCP et UDP et TCP / IP.

Couche Session : S'occupe de fiabiliser la communication utilisateurs, gère des tours de parole, synchronisation. Synchronisation du Dialogue

Couche Présentation : Assure une transparence en termes de codage (ex. ASCII). Représentation des structures de données

Couche Application : Gère les applications de types réseaux : courrier électronique, transfert de fichier, appel de procédures distantes...et d'autres applications Normalisées (FTAM, JTM, MHS,...)

Figure 1.4: Communication entre couches.



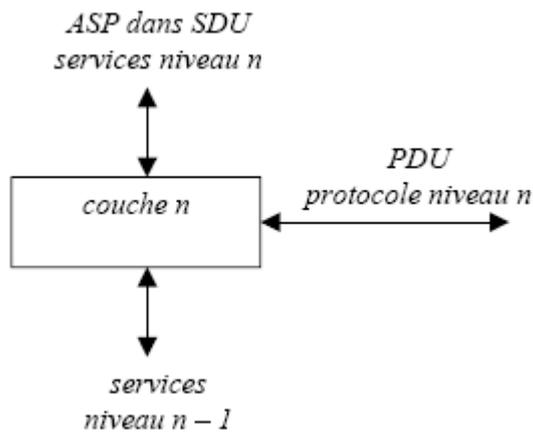
Chaque couche est constituée d'éléments matériels et logiciels et offre un service à la couche située immédiatement au-dessus d'elle en lui épargnant les détails d'implémentation nécessaires. Comme illustré dans la figure 1.4, chaque couche n d'une machine gère la communication avec la couche n d'une autre machine en suivant un protocole de niveau n qui est un ensemble de règles de communication pour le service de niveau n.

En fait, aucune donnée n'est transférée directement d'une couche n vers une autre couche n, mais elle l'est par étapes successives. Supposons un message à transmettre de l'émetteur A vers le récepteur B. Ce message, généré par une application de la machine A va franchir les couches successives de A via les interfaces qui existent entre chaque couche pour finalement atteindre le support physique.

Là, il va transiter via différents noeuds du réseau, chacun de ces noeuds traitant le message via ses couches basses. Puis, quand il arrive à destination, le message remonte les couches du récepteur B via les différentes interfaces et atteint l'application chargée de traiter le message reçu. Ce processus de communication est illustré dans la figure 1.5.

Protocole et service

Encapsulation des services couche par couche.



- **ASP** (Abstract Service Protocol) dans **SDU** (Service Data Unit) : Les primitives de service ASP classiques sont CON, DIS, DT.

- **PDU** (Protocol Data Unit) : Les entités de protocole PDU classiques sont CR,CC, AR, DR, DC, DATA.

Nous allons maintenant détailler les caractéristiques de chacune de ces couches en précisant d'abord que les fonctions et services définis dans les couches du modèle OSI peuvent se retrouver dans d'autres couches dans les systèmes opérationnels disponibles sur le marché. Il se peut également qu'une fonctionnalité localisée dans une seule couche dans le modèle OSI se retrouve répartie sur plusieurs couches.

Mais cela illustre simplement la distance qui existe entre un modèle théorique et ses implantations

Chapitre 2 : La Couche physique :

Définition :

La couche physique fournit les moyens mécaniques, électriques, fonctionnels et procéduraux nécessaires à l'activation, au maintien et à la désactivation des connexions physiques destinées à la transmission de bits entre deux entités de liaison de données.

Ici, on s'occupe donc de transmission des bits de façon brute, l'important est que l'on soit sûr que si l'émetteur envoie un bit à 1 alors le récepteur reçoit un bit à 1. Les normes et standards de la couche physique définissent le type de signaux émis (modulation, puissance, portée...), la nature et les caractéristiques des supports (câble, fibre optique...), les sens de transmission...

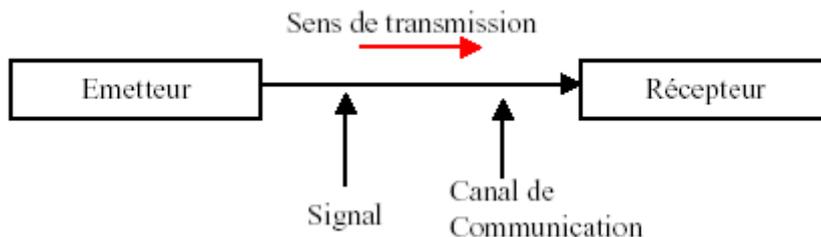
La transmission de plusieurs bits peut s'effectuer en *série* ou en *parallèle*.

I – Codage de l'information : Les réseaux de données ont pris naissance dans la numérisation des informations. Le codage des informations par des 0 et des 1. Plusieurs codes normalisés existent. Les principaux codes sont :

le code ASCII, le code EBCDIC et Télégraphique.

II – Notion de transmission : Une fois le codage des données est fait , il faut transmettre ses bits sur le réseau.

II – 1. Système de communication

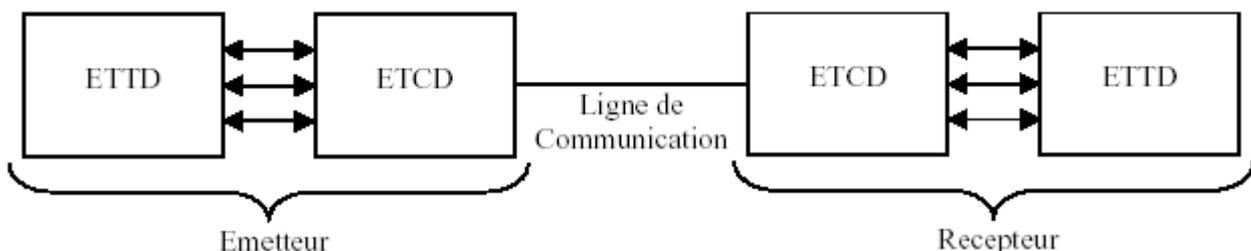


Problème de la transmission : Trouver une bonne transformation de l'information de signal tel que le canal soit capable de le propager correctement.

II – 2. Système de communication informatique

Dans le cas de système informatique, l'information à transmettre est une suite de bits et les éléments composants le bipoint du système sont :

- Les ETTD (Equipement Terminal de traitement de donnée, Ordinateurs, PC, imprimante, ...).
- Les ETCD (Equipement Terminal de circuit de Donnée) : Equipements permettent de transformer les bits en signaux (modem).



II – 3 Nature des liaisons de données

➤ **La direction de la communication**

Tout d'abord une liaison entre 2 équipements A et B peut être *simplex* (unidirectionnelle), dans ce cas A est toujours l'émetteur et B le récepteur. C'est ce que l'on trouve par exemple entre un banc de mesure et un

ordinateur recueillant les données mesurées. La communication est *half-duplex* (bidirectionnelle à l'alternat) quand le rôle de A et B peut changer, la communication change de sens à tour de rôle (comme avec des talkies-walkies). Elle est *full-duplex* (bidirectionnelle simultanée) quand A et B peuvent émettre et recevoir en même temps (comme dans le cas du téléphone).

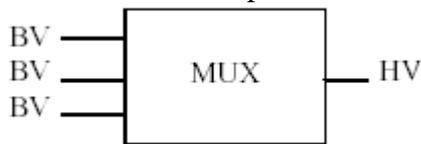
- **Simplex** : Transmission dans un seul sens.
- **Semi – Duplex** : Transmission dans les 2 sens mais alternativement.
- **Duplex** : Transmission dans les 2 sens simultanément.

Configuration des liaisons de données

- **Liaison point à point** : Deux ETTD reliés. Une suite de liaisons point à point forme un anneau.
- **Liaison multi – point** : La même liaison est partagée entre plusieurs ETTD.

III – Multiplexeurs

Lorsque plusieurs circuits de données existent, il est intéressant de concentrer les données transmises sur des voies de basse vitesse (BV) sur un seul circuit de donnée à plus fort débit (HV). Multiplexeurs et concentrateurs réalisent cette opération.



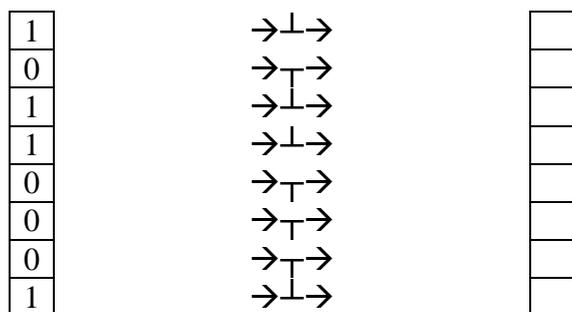
- **Multiplexage en fréquence** : Chaque voie BV conserve sa BP sur la voie HV.- La voie HV doit avoir une capacité suffisante pour absorber toutes les données provenant des voies BV.
- **Multiplexage temporel** : Suit le même mécanisme, mais au lieu de diviser la voie HV en fréquences, on découpe le temps en tranches affectées régulièrement à chaque voie.

IV – la nature de la communication

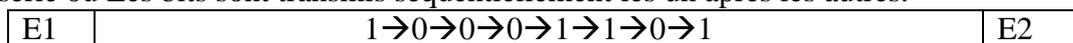
IV – 1. Transmission série et parallèle

La transmission de bit peut – être faite de deux manières :

- **En parallèle** : Transmission de plusieurs bits simultanément (bus d'un micro de 8 ou 16 bits). Plusieurs communications simultanément. Il peut être intéressant, notamment lorsque les ETTD sont séparés par une courte distance (moins d'un mètre), chaque bit est transféré sur une ligne à part. cela aura pour effet de réduire le délai de transfert.



- **En série** : lorsque la distance séparant les ETTD dépasse quelques mètres , la transmission en parallèle ne peut plus être utilisée pour des raisons de coût mais également pour des difficultés de mise en œuvre inhérentes au délai de propagation qui peut varier d'une ligne à l'autre. On utilise alors la transmission en série où Les bits sont transmis séquentiellement les un après les autres.



La conversion de la forme parallèle vers la forme séquentielle se fait par des registres à décalage



IV – 2. Synchronisation

On appelle rapidité de modulation (baud rate) d'un signal ou d'un canal le nombre d'impulsions pouvant être véhiculées par unité de temps. La rapidité de modulation qu'on notera R peut s'exprimer en fonction de T par la relation $R=1/T$ ou T =la durée matérialisant la transmission d'un bit. La valeur de R est limitée par la qualité du canal et la capacité de lecture du récepteur.

On appelle débit binaire d'un signal ou d'un canal, et on note D , le nombre de bits pouvant être véhiculés par unité de temps. Pour un signal à deux niveaux $D=R$, lorsque les données sont représentées par un signal à plusieurs niveaux le débit est donné par la formule $D=R \log_2 V$ ou V exprime la valence ou le nombre de niveaux du signal D est exprimé en bit/seconde.

Pour que l'ETTD récepteur puisse identifier chaque bit lors de la réception d'une séquence quelconque de bits, il est nécessaire qu'il connaisse la rapidité de modulation du signal véhiculant ces bits. On dit que l'ETTD émetteur et l'ETTD récepteur sont synchronisés au niveau bit.

Si l'unité de transfert est l'octet alors le récepteur doit être en mesure de reconnaître le début et la fin de chaque caractère et on dit que l'émetteur et le récepteur sont synchronisés au niveau caractère.

Si l'unité de transfert est le bloc alors le récepteur doit être en mesure de reconnaître le début et la fin de chaque bloc et on dit que l'émetteur et le récepteur sont synchronisés au niveau bloc.

On distingue généralement deux techniques de synchronisation : technique asynchrone et technique synchrone.

La technique asynchrone est mise en œuvre entre un émetteur et un récepteur disposant d'horloge indépendantes ce qui donne à l'émetteur la possibilité d'émettre à tout moment.

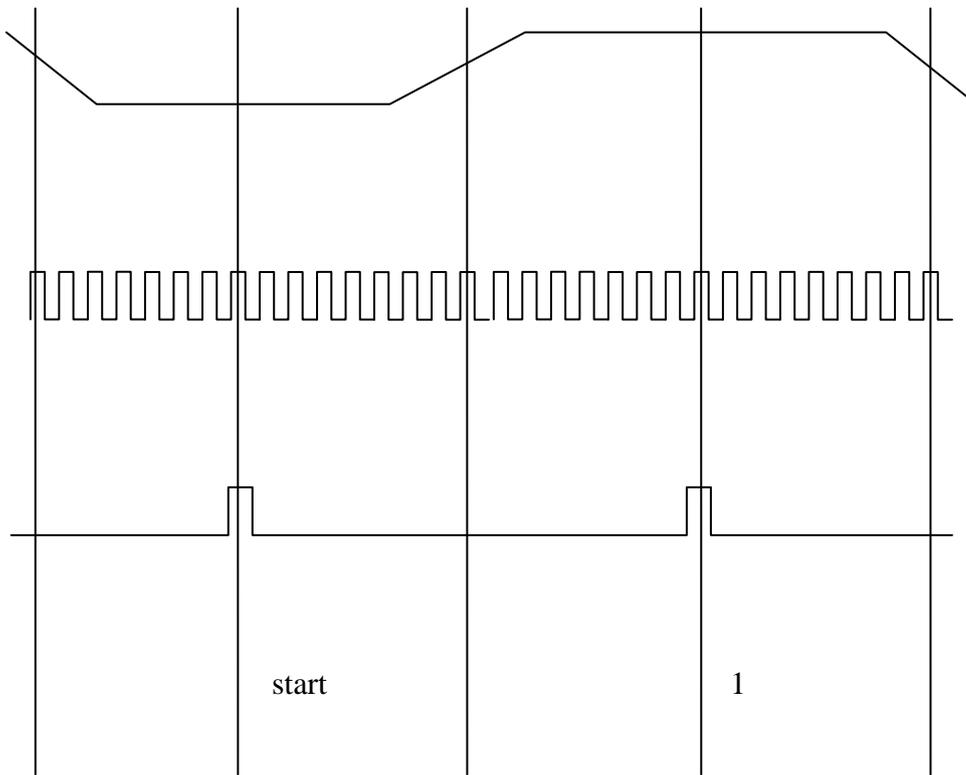
La technique synchrone par contre est mise en œuvre entre un émetteur et un récepteur disposant d'un même référentiel temporel.

a) Transmission asynchrone

- Les caractères sont transmis de façon irrégulière (clavier, ...).
- L'intervalle entre 2 caractères est aléatoire.
- Le début du message peut arriver à n'importe quel moment. Mais il faut reconnaître le début et la fin d'un caractère pour permettre la synchronisation bit intra caractère. Ce qui se fait par l'ajout des bit -start et bit-stop .

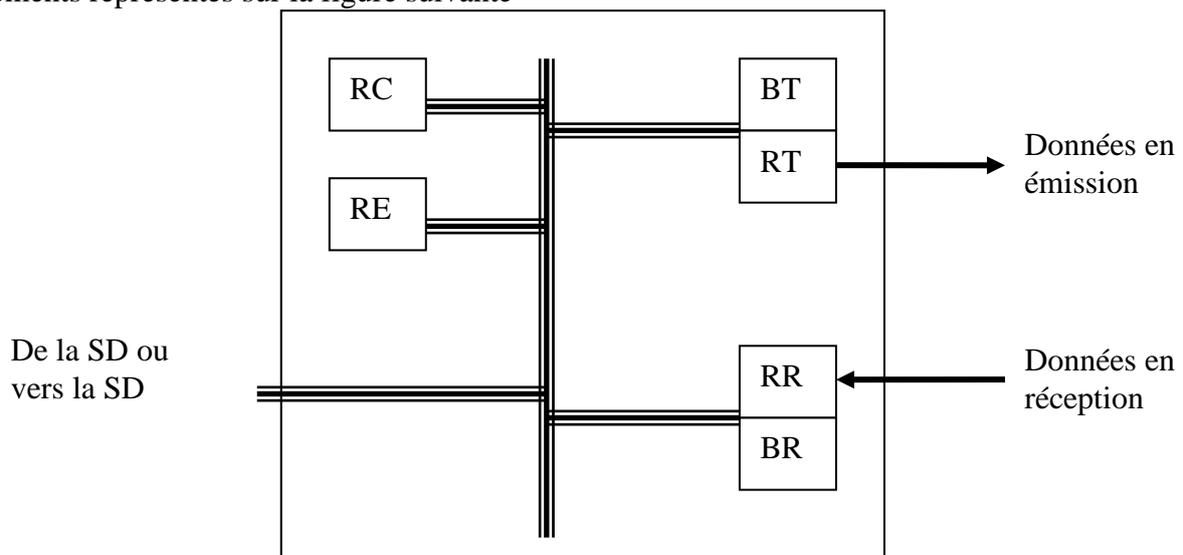


La synchronisation entre émetteur et récepteur se fait de la manière suivante le bit start provoque une transition entre l'état logique 1 (état de repos) et l'état logique 0 et signal ainsi au récepteur l'arrivée d'un nouveau caractère. Le récepteur, qui connaît la rapidité de modulation, utilise une horloge dont la fréquence est n fois plus grande que la rapidité de modulation du signal représentant le caractère. N étant généralement choisi égale à 16. ce grandeur permet au récepteur d'échantillonner avec précision le signal reçu au milieu de chaque impulsion



Echantillonnage du signal reçu par le récepteur.

- Le premier graphe représente le bit start suivi de bit 1.
- Le deuxième graphe représente le signal d'horloge (au moment élémentaire du signal reçu correspond 16 périodes d'horloge).
- Le troisième graphe représente le signal d'échantillonnage. : le récepteur qui scrute le canal initialise à 8 un compteur modulo 16 dès la détection de la première transition du signal de l'état de repos vers l'état logique 0 (début du bit start) . chaque remise à zéro du compteur par la suite va générer un signal échantillonnant en plein milieu chaque impulsion.
- Pour réaliser des transmission asynchrones on utilise des interfaces de communication appelées UARTs (universal asynchronous receiver and transmitter). Une UART est un circuit intégré composé des éléments représentés sur la figure suivante



- **RC** : registre de contrôle.
- **RE** : registre d'état .
- **BT**: buffer de transmission . >asw
- **RT** : registre de transmission .

- **RR** : registre de réception .
- **BR** : buffer de réception.

Le circuit est dit universel du fait qu'il est programmable l'utilisateur peut, grâce au registre de contrôle programmer :

- Le nombre de bits par caractère (généralement 5,6,7 ou 8 bits).
- Le type de parité (paire , impaire , ou nulle)
- Le nombre de bits stop (généralement 1,1 et ½, ou 2).
- Le débit binaire (typiquement 110 , 300 , 1200 , 2400, 4800, 9600, et 19200).

Le registre d'état se compose d'indicateurs portant les noms suivants :

- Buffer de transmission vide (ou BTV)
- Buffer de réception plein (BRP)
- Indicateur d'erreurs (erreur de parité ou EP ; erreur d'encadrement ou EEN, erreur d'écrasement EEC).

BTV =1 → le caractère précédent a été transféré du buffer de transmission vers le registre de transmission , la source de donnée (SD) peut alors charger un nouveau caractère dans le buffer de transmission ,

Le bit start et le bits stop sont ajoutés au caractères après son transfert dans le registre de transmission. Lorsque tout le caractère (bits de données plus parité) est disponible au niveau du registre de réception, il est transféré en parallèle dans le buffer de réception , après est recalculé du bit de parité , l'indicateur BRP et éventuellement l'indicateur EP sont mise à 1.

L'indicateur EEn=1 → la valeur du dernier bit stop n'est pas la valeur attendu (0 au lieu 1).

L'indicateur EEC =1 → le caractère en attente de prélèvement dans le buffer de réception n'a pas été prélevé à temps et qu'il a été écrasé par un autre caractère en provenance du registre de réception.

Les avantages de la transmission asynchrone :

- Simple à mettre en œuvre,
- Peu coûteuse,
- Débit limité.

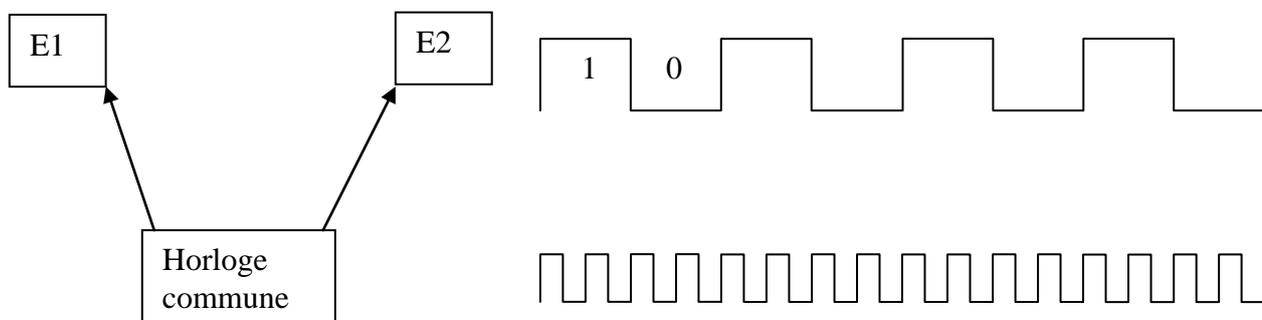
b) Transmission synchrone

Est utilisée lorsque le flux de données est régulier sans séparation entre les caractères. Et notamment lorsque les quantités d'informations à transférer sont importantes. Dans ce cas il serait trop coûteux d'envoyer des informations de synchronisation avec chacun des caractères. Pour cela, émetteur et récepteur possèdent un référentiel temporel commun, qui peut être mis en œuvre par différents procédés.

la synchronisation : c'est le fonctionnement de l'émetteur et du récepteur avec le même référentiel temporel.

b-1) horloge d'un système maître :

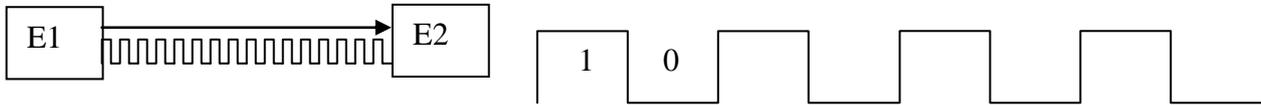
Une horloge placée au niveau d'un système maître pourrait imposer à l'émetteur l'instant de dépôt de chaque information et au récepteur l'instant de prélèvement de cette information.



L'instant de dépôt pourrait correspondre au front de l'impulsion du signal d'horloge alors que l'instant de prélèvement pourrait correspondre à la queue de l'impulsion.

b-2) horloge pilotée par l'émetteur :

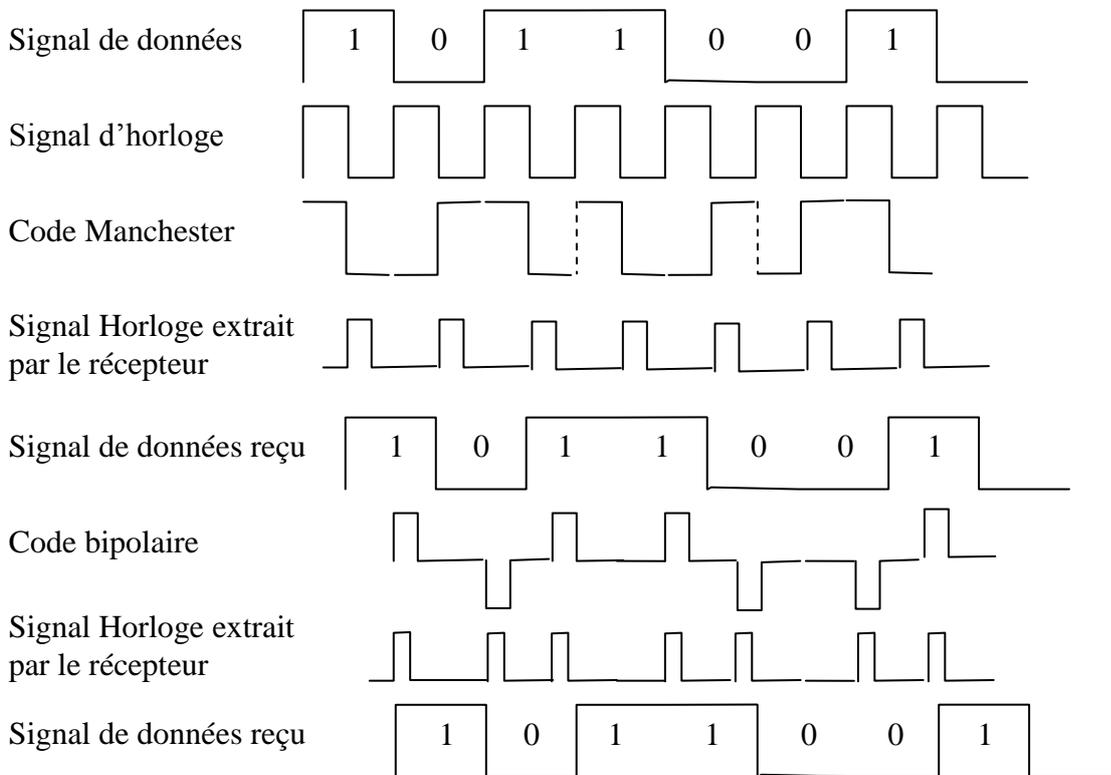
sur le plan du principe, ce procédé de mise en œuvre est le même que le précédent. En effet la seule différence avec la précédente est que dans ce cas l'émetteur joue le rôle d'émetteur et d'horloge commune , mais pour des raisons des problèmes lies a la transmission parallèle , les deux procédés présentes ne sont applicables que sur des distances courtes.



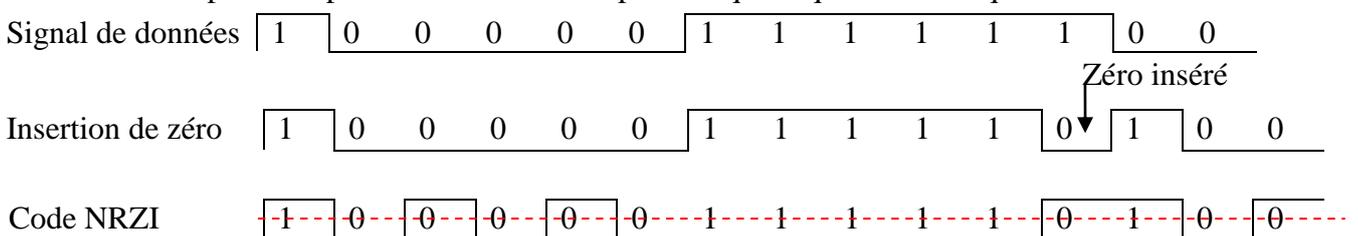
b-3) auto-synchronisation :

dans le cas où les deux ETTD's sont séparées par de longues distances, il est évident qu'il est impossible d'utiliser une horloge commune , il est plus convenable de :

- Premièrement : combiner le signal d'horloge et le signal de données sur le même canal, et de les séparer à l'arrivée. (par exemple le code manchester ou le code bipolaire voir la figure)



- Deuxièmement : utiliser un signal pour les données qui contient suffisamment de transitions , ce qui permettra à l'ETTD récepteur de maintenir en synchronisation permanente une horloge qui lui est propre . une manière d'obtenir un signal contenant suffisamment de transitions, consiste à utiliser le code NRZI (no return to zero inverted) combiné à l'insertion d'un zero après une séquence de 1 consécutives par exemple le HDLC insert 0 après chaque séquence de cinq 1 consécutifs.



pour garder la synchronisation entre le récepteur et l'émetteur après pendant la réception des grands blocs de données sans bit Start et bits Stop, il faut recalibrer (régler) l'horloge du récepteur suite de chaque transition de données reçus.

L'idée de base consiste à utiliser, au niveau du récepteur une horloge de fréquence n fois plus élevée que la rapidité de modulation du signal véhiculant les données. n qui est choisi égale à 32.

Permet au récepteur d'échantillonner le signal reçu avec exactitude au milieu de chaque moment élémentaire. si la transition arrive avant la transition il diminue la fréquence de l'horloge et dans le cas contraire il va augmenter l'horloge.

V – Différents modes de transmission

V – 1. Transmission en bande de base

- Il n'est pas nécessaire de moduler le signal après codage.
- Le signal émis sur la ligne est celui obtenu après le codage.
- L'intérêt de ce codage est le coût peu élevé.

Remarque :

Les signaux bande de base sont sujets à une atténuation dont l'importance dépend du support. Ils doivent être régénérés périodiquement, en utilisant des répéteurs.

Répéteur : Mémoire une fraction de seconde les signaux avant de le retransmettre sur la ligne sortante.

Différents codages : voir TD (code NRZ, biphase de Manchester, biphase différent, ...).

Transmission en bande de base.

La transmission en bande de base consiste à envoyer directement la suite de bits sur le support à l'aide de *signaux carrés* constitués par un courant électrique pouvant prendre 2 valeurs (5 Volts ou 0 par exemple). On détaillera ci-après les différents codages des bits possibles, mais dans tous les cas l'émetteur envoie sur la ligne un signal carré du type de celui de la figure 1.6 pour la séquence de bits 1010 par exemple.

Figure: Signal carré de la séquence de bits 1010.

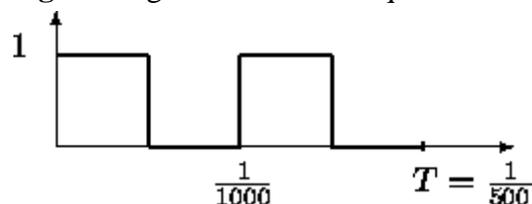
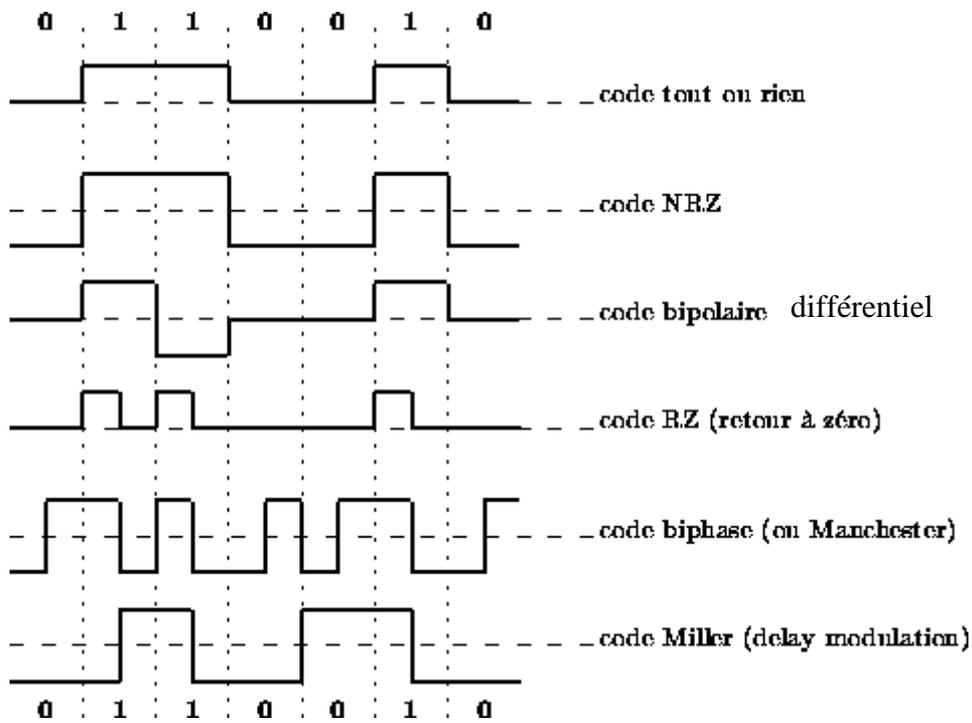


Figure: Différents codages en bande de base de la séquence 0110010.



1.8

- le *code tout ou rien* : c'est le plus simple, un courant nul code le 0 et un courant positif indique le 1
- le *code NRZ* (non retour à zéro): pour éviter la difficulté à obtenir un courant nul, on code le 1 par un courant positif et le 0 par un courant négatif.
- le *code bipolaire* : c'est aussi un code tout ou rien dans lequel le 0 est représenté par un courant nul, mais ici le 1 est représenté par un courant alternativement positif ou négatif pour éviter de maintenir des courants continus.
- le *code RZ* : le 0 est codé par un courant nul et le 1 par un courant positif qui est annulé au milieu de l'intervalle de temps prévu pour la transmission d'un bit.
- le *code Manchester* : ici aussi le signal change au milieu de l'intervalle de temps associé à chaque bit. Pour coder un 0 le courant sera négatif sur la première moitié de l'intervalle et positif sur la deuxième moitié, pour coder un 1, c'est l'inverse. Autrement dit, au milieu de l'intervalle il y a une transition de bas en haut pour un 0 et de haut en bas pour un 1.
- le *code Miller* : on diminue le nombre de transitions en effectuant une transition (de haut en bas ou l'inverse) au milieu de l'intervalle pour coder un 1 et en n'effectuant pas de transition pour un 0 suivi d'un 1. Une transition est effectuée en fin d'intervalle pour un 0 suivi d'un autre 0.

➤ Tout ou Rien :

Si $(e=0)$ alors $s(t)=0v$

Sinon $(e=1)$ alors $s(t)=5v$

➤ NRZ:

Si $(e=0)$ alors $s(t)=-5v$

Sinon $(e=1)$ alors $s(t)=+5v$

➤ RZ:

Si $(e=0)$ alors $s(t)=0v$

Sinon $(e=1)$ alors $[0, T/2] s(t)=+5v$, $]T/2, T[s(t)=0v$

➤ Code bipolaire:

Si $(e=0)$ alors $s(t)=0v$

Sinon

$$\begin{cases} \text{si } (s(t-1) = 0 \text{ ou } s(t-1) = \text{null alors } s(t) = +5v \\ \text{si non } s(t) = -s(t-1) \end{cases}$$

➤ Code Manchester:

Si (e=0) alors

$$\begin{cases} \left[0, \frac{T}{2}\right] s(t) = -5v \\ \left[\frac{T}{2}, T\right] s(t) = +5v \end{cases}$$

Sinon

$$\begin{cases} \left[0, \frac{T}{2}\right] s(t) = +5v \\ \left[\frac{T}{2}, T\right] s(t) = -5v \end{cases}$$

➤ Code Miller:

Si (e=0) alors

$$\begin{cases} \text{si } s(t-1) = \text{null alors } s(t) = -5v \\ \text{si non } \begin{cases} \text{si } s(t-1) = 0 \text{ alors } s(t) = -s(t-1) \\ \text{sinon } s(t) = s(t-1) \end{cases} \end{cases}$$

Sinon

$$\begin{cases} \text{si } s(t-1) = \text{null alors } \begin{cases} \left[0, \frac{T}{2}\right] s(t) = +5v \\ \left[\frac{T}{2}, T\right] s(t) = -5v \end{cases} \\ \text{si non } \begin{cases} \left[0, \frac{T}{2}\right] s(t) = s(t-1) \\ \left[\frac{T}{2}, T\right] s(t) = -s(t-1) \end{cases} \end{cases}$$

VI – 2. Transmission large bande

Pour transmettre l'information a longue distance, on module une onde porteuse sinusoïdale.

Mathématiquement, elle est de la forme : $s(t) = A \cdot \sin(\omega.t + \Phi)$ A : Amplitude , ω : Pulsation , Φ : Phase initiale ou $s(t) = A \cdot \sin(2\pi f.t + \Phi)$ f : Fréquence

Les types de modulation :

- **Modulation d'amplitude** : Le signal est modulé en faisant varier l'amplitude.

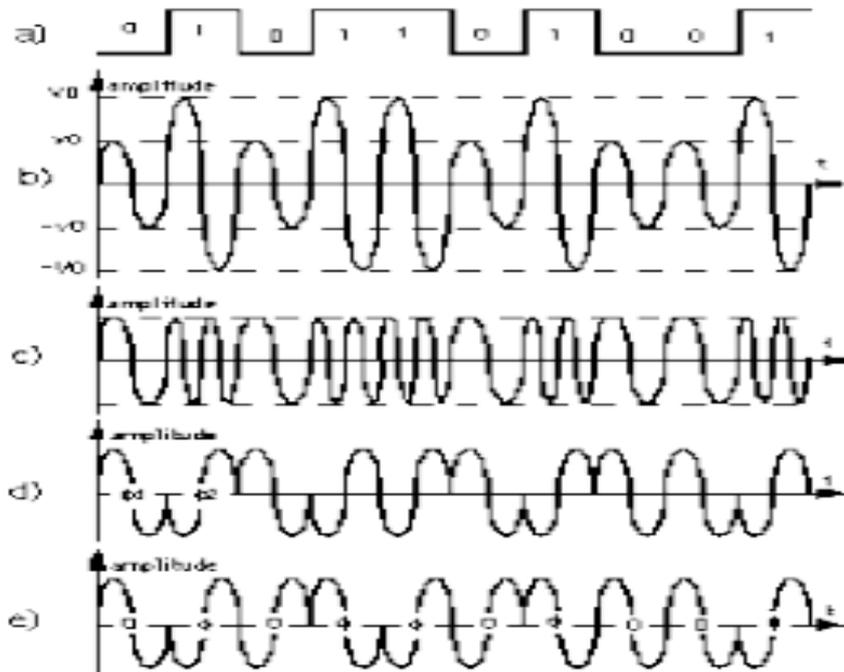
$$s(t) = A(t) \cdot \sin(\omega.t + \Phi)$$

cette technique est efficace si la bande passante et la fréquence sont bien ajustées par contre , il existe des possibilités de perturbation (orage, lignes électriques..) car si un signal de grande amplitude (représentant un 1) est momentanément serais affaibli le récepteur l'interprétera à tort en 0.

- **Modulation de fréquence** : $s(t) = A \cdot \sin(2\pi f(t).t + \Phi)$, c'est un signal très résistant aux perturbations (la radio FM est de meilleur qualité que la radio AM) et c'est assez facile à détecter.
- **Modulation de phase** : $s(t) = A \cdot \sin(2\pi f.t + \Phi(t))$
- **Modulation hybride** : une modulation où il possible de faire varier plusieurs paramètres de la porteuse à la fois. Ce type de modulation à pour objectif d'augmenter le nombre d'informations élémentaires transmises durant un cycle de la porteuse.

Exemple de modulation hybride entre amplitude et phase

$$00 : p\sin(\omega t) \quad , \quad 01 : p\sin(\omega t + \pi) \quad 10 : p/2\sin(\omega t) \quad , \quad 11 : p/2\sin(\omega t + \pi)$$



Le principal problème de la transmission en bande de base est la dégradation du signal très rapide en fonction de la distance parcourue, c'est pourquoi elle n'est utilisée qu'en réseau local (<5km). Il serait en effet trop coûteux de prévoir des répéteurs pour régénérer régulièrement le signal. C'est pourquoi sur les longues distance on émet un signal sinusoïdal qui, même s'il est affaibli, sera facilement décodable par le récepteur.

Ce signal sinusoïdal est obtenu grâce à un modem (modulateur-démodulateur) qui est un équipement électronique capable de prendre en entrée un signal en bande de base pour en faire un signal sinusoïdal (modulation) et l'inverse à savoir restituer un signal carré à partir d'un signal sinusoïdal (démodulation). Autrement dit il permet de passer de signaux numériques discrets (0 ou 1) à des signaux analogiques continus.

Il existe trois types de modulation décrits ci-dessous :

1_ la modulation d'amplitude envoie un signal d'amplitude différente suivant qu'il faut transmettre un 0 ou un 1. Cette technique est efficace si la bande passante et la fréquence sont bien ajustées.

Par contre, il existe des possibilités de perturbation (orage, lignes électriques...), car si un signal de grande amplitude (représentant un 1) est momentanément affaibli le récepteur l'interprétera à tort en un 0.

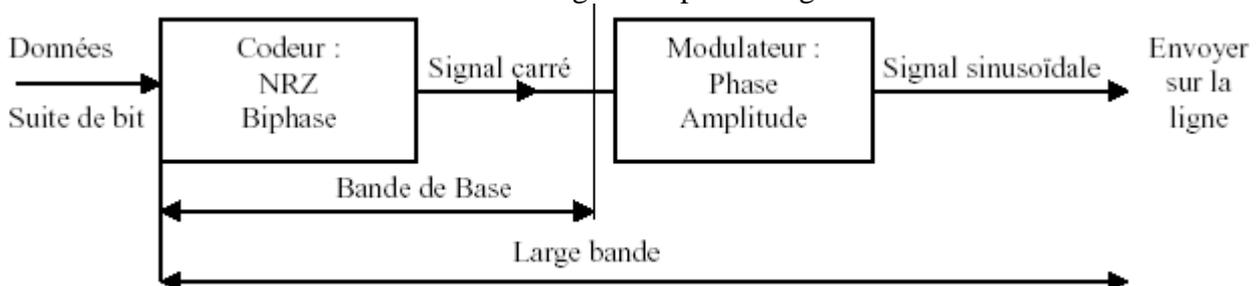
2_ la modulation de fréquence envoie un signal de fréquence plus élevée pour transmettre un 1. Comme l'amplitude importe peu, c'est un signal très résistant aux perturbations (la radio FM est de meilleure qualité que la radio AM) et c'est assez facile à détecter.

3_ la modulation de phase change la phase du signal (ici de 180_) suivant qu'il s'agit d'un 0 (phase montante) ou d'un 1 (phase descendante).

VII – Les modems

VII – 1. Le modem émetteur

Transforme les données à émettre en un signal adapté à la ligne.



Remarque :

Dans la transformation en bande de base, l'appareil transforme les données .

Ne fait pas de modulation. Dans ce cas, on l'appelle plutôt "transceiver" ou transmetteur.

VII – 2. Le modem récepteur



VII – 3. Normalisation des modems

Les modems et les interfaces sont normalisés ce qui assure une bonne compatibilité entre les équipements. Le classement des modems se fait en fonction des critères suivants:

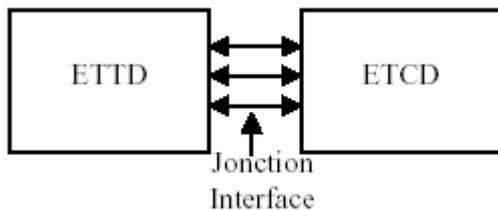
- **Technique de transmission** : bande de base, large bande.
- **Débit** : 300 bit/s, 600 bit/s, ..., 1200 bit/s.
- **Support de transmission** : réseau commuté, ligne spécialisé, ligne semi-duplex et duplex.
- **Méthode de synchronisation** : asynchrone, synchrone.
- **Format de l'appareil** : Boîtier indépendant, carte à insérer dans un ordinateur.

Il en résulte plus d'une vingtaine de modems normalisés.

VII – 4. Jonction modem – Terminal (ETTD – ETCD)

L'interface est définie essentiellement par des caractéristiques mécaniques électriques, fonctionnelles et procédurales :

- ❖ Les caractéristiques mécaniques : le type de connecteurs, la forme,etc
- ❖ Les caractéristiques électriques : les niveaux de tension, la cadence de communication.
- ❖ Les caractéristiques fonctionnelles : fonction de chaque circuit "transfert de données, contrôle de données, ... etc.
- ❖ Les caractéristiques procédurales : la séquence des différents événements.



Pour accéder à un circuit de donnée, il faut réaliser les étapes suivantes :

- Etablissement du circuit (si la ligne n'est pas affectée en permanence).
- Initialisation (adapter le modem à la ligne).
- Transmission des données.
- Libération de circuit.

Les standards RS-232-c:

Standard de l'EIA (Electrical industrial Association).

Destinés pour des modem (ou autre) travail avec des lignes analogiques et des débit pouvant atteindre les 19200 bps, sur des distances relativement courtes

Avis X.21 du CCITT

Définit pour les interfaces de communication synchrone pour l'accès aux réseaux publics de transmission de données.

Avis V24

Cette interface définit la séquence logique des opérations effectuées à la jonction ETTD – ETCD, en décomposant celle – ci en autant de fils, de fonction d'échanges à réaliser. Les différents circuits sont numérotés.

Ex. : Dans la série 100 les principaux circuit numérotés :

102 => Masse

103 => Emission de donnée

104 => Réception

105 => Demande pour émettre

106 => Prêt à émettre

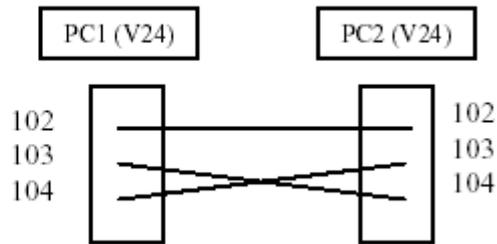
108 => Réception prêt

Application

Connexion de deux PC sans modem. On veut donc réaliser une connexion directe ETTD –ETTD.

V24 croisé

Null Modems



Algorithme:

Procédure – Emettre (Message)

```
    Pour i de 1 à long (Message)
    |   Faire émettre (Message [i])
    |   Fait
    Emetteur (car_fin_de_Message)
```

Fin

Procédure – Recevoir (Message)

```
    Message = ‘ ‘;
    Répéter
    |   Recevoir (c)
    |   Si c != car_fin_de_Message
    |   |   Alors Message <= Message c
    |   Finsi
    Jusqu’à c = car_fin_de_message
```

Fin

Les registres de V24 sont :

THR : Registre d’écriture

RBR : Registre de lecture

LCR : Lire Control Register

LSR : Lire Status Register

Procédure – Emettre (c)

```
    Tant que je ne suis pas autorisée à émettre
    |   Attendre;
    Fin tant que
    Ecrire c dans THR
```

Fin

Procédure – Recevoir (c)

```
    Tant que je ne suis pas autorisé à lire
    |   J’attends;
    Fin tant que
    C <= contenu du registre RBR
```

Fin

VIII – Le réseau téléphonique pour la transmission de donnée

VIII – 1. Utilisation du réseau commuté

Le réseau commuté peut transmettre des données mais à un débit de 4500 bit/s. Le réseau est accédé depuis l’ETTD via un modem normalisé pour respecter les caractéristiques du réseau.

Intérêt : Atteindre des correspondants situés n’importe où. Le coût de communication est environ égale au coût de la communication téléphonique.

VIII – 2. Le RNIS

Réseau Numérique à Intégration de Service.

Le RNIS se caractérise par la distribution jusque chez l'abonné des canaux déjà présent dans le réseau actuel.

- L'utilisateur a accès non seulement au réseau téléphonique, mais à un réseau de transmission apte à véhiculer le son, l'image et les données.

Principe du RNIS : Accès de base de 144 Kbits et comporte 2 voies de 64 Kbits et 1 voie de 16 Kbits.

Les canaux B permettent de téléphoner tout en envoyant un fichier. Les canaux sont réservés aux transferts liés aux informations de service.

Remarque : Pour accéder aux réseaux numériques, il faut une interface standard de type X21.

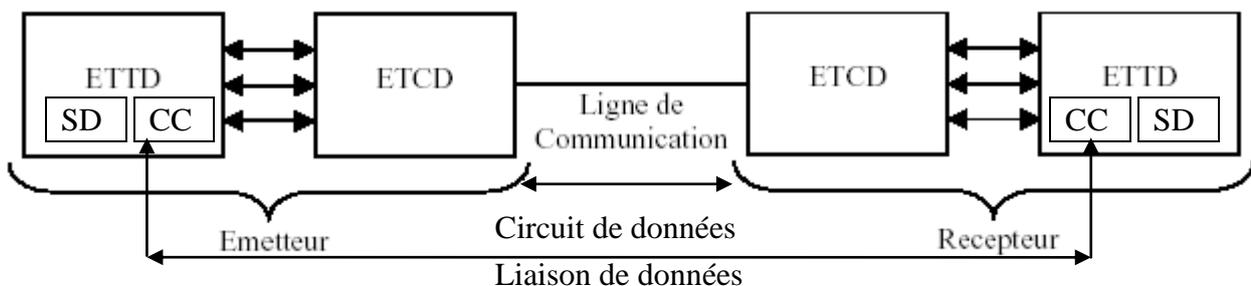
Pour ne pas jeter les micros munis uniquement de V24, on passe par un convertisseur X21 bis.

Chapitre 3 : La Liaison de données :

4-1-Définition : La couche liaison de données fournit les moyens fonctionnels et procéduraux nécessaires à l'établissement, au maintien et à la libération des connexions de liaison de données entre entités du réseau. Elle détecte et corrige, si possible, les erreurs dues au support physique et signale à la couche réseau les erreurs irrécupérables. Elle supervise le fonctionnement de la transmission et définit la structure syntaxique des trames, la manière d'enchaîner les échanges selon un protocole normalisé ou non. Une liaison de données est réalisée à l'aide d'une ou plusieurs liaisons physiques entre deux machines adjacentes dans le réseau donc sans nœuds intermédiaires entre elles.

4-2-Objectifs de la couche liaison de données :

- Que les blocs échangés soient structurés selon des formats standards et clairement délimités. –afin de les reconnaître et les interpréter- exp : bit start et 2 bits stop.
- Implémentation d'un mécanisme de détection d'erreur , et éventuellement une stratégie de correction d'erreur . exp : bit de parité.
- Asservir l'émetteur à la capacité d'absorption du récepteur , le mécanisme de régulation de flux pour assurer une exploitation optimale du canal et pour l'évitement d'erreur d'écrasement.
- Prévoir une procédure de dialogue entre l'émetteur et le récepteur . exp : protocole de liaison –HDLC-.



SD : Source de données.

CC : Contrôleur de communication
Spécification

4-3-Définition d'une trame :

Tout bloc de données échangé au niveau d'une liaison de données. Le format d'une trame dépend du type de protocole de liaison de données.

Il y a deux type de protocoles de liaison synchrone comme (HDLC) , et asynchrone comme(ATM).

4-3-1 Protocoles Synchrones :

Il y a deux types de protocoles de liaison synchrone :

a- Basé sur le caractère (COP : Character Oriented Protocol).

b- Basé sur le bit (BOP : Bit Oriented Protocol).

a- Format de trame pour protocole basé sur le caractère :

Il s'agit de trames formées d'un nombre entier d'octets généralement variable.

Soit l'exemple d'une trame de protocole BSC d'IBM (Binary synchronous contrôle)

SYN	SYN	SOH	HEADER	STX	DONNEES	ETX	BCC
-----	-----	-----	--------	-----	---------	-----	-----

SYN , SOH ,STX ,ETX : sont des caractères réservés choisis parmi les caractères du code ASCII

SYN : caractère de synchronisation , il précède toute émission de nouvelle trame.

SOH : (start of header) début d'entête.

Header : un entête compose généralement d'une adresse du récepteur et le N° d'ordre de séquence de trame

STX : (start of text) indique le début des données utiles.

ETX : (end of text) indique la fin de données utiles.

BCC : (Block check charcter) est un caractère utilisé pour le contrôle d'erreur .

Si le champ données contient un caractère de contrôle il ya un risque de fausse interprétation pour assurer la transparence de la transmission il faut insérer un caractère « DLE : data link escape).

b- B-Format de trames basées sur le bit :

Basée sur le bit , il n'est pas exigé que la trame soit constituée d'un nombre entier d'octets , par exemple le protocole HDLC .(high level datal link control):

Est apparu en 1976 pour répondre aux besoins de communiquer un terminal avec une machine distante.

HDLC améliore les protocoles basés sur transmission synchrone c-à-d envoi de message et attente d'acquiescement en procédant à la retransmission par anticipation , l'attente de l'acquiescement n'empêche pas la transmission des trames suivantes :

Flag	Header	Information	FCS	FLag
1oct	2oct			

- Le champ FLAG (fanion) est constitué d'un octet (01111110) servant à délimiter la trame.
- Le champ HEADER un entête constitué de deux octets : le premier octet correspond à une adresse et le second octet à une commande.
- Le champ FCS : (Frame Check Sequence) codé sur deux octets et sert au contrôle d'erreur.

Pour assurer la transparence de la transmission des données chaque séquence consécutive de cinq(1) nécessite l'insertion automatique d'un zéro.

c- Types de messages de l'HDLC:

- ❖ Les trames I: (informations).
- ❖ Les trames S (Supervision).
- ❖ Les trames U (unumbred , nom numérotées trames de gestion).

Les trames I: transportent les informations en provenance de la couche supérieure chaque trame I , contient le numéro N(s) de la trame , le numéro N(r) indiquant la prochaine trame attendue par le récepteur , N(r) joue le rôle d'un accusé de réception positif en indiquant que toutes les trames ayant un numéro inférieur à N(r) ont bien été reçus .

Les trames S: elles permettent le transport des commandes sont au nombre de quatre

- 1- la trame RR (receiver Ready).porte des acquiescements qui ne sont pas émis dans une trame I.
- 2- la trame RNR (receiver not ready) donne un contrôle de flux de niveau trame en demandant à l'émetteur de stopper les envois jusqu'à la réception d'une nouvelle trame RR spécifiant le même numéro.
- 3- La trame REJ(reject) correspond à la reprise sur erreur en cas de détection d'anomalies.
- 4- La trame SREJ(selective reject) correspond à la reprise sur erreur en cas de détection d'anomalies.

Les trames U: sont utilisés pour effectuer les fonctions de commande de la liaison et pour le transfert d'informations non numérotées.

Exp :

- SABM :** (mise en mode asynchrone équilibré)
- Disc:** (déconnexion)
- DM:** (mode déconnecté)
- UA :** (accusé de réception non numéroté).
- FRMR :** (rejet de trame)

4-4-Protection contre les erreurs de transmission :

On vue que le bruit environnant et le bruit blanc exercent des effets indésirables sur les données transmises , pouvaient se traduire au niveau liaison par l'altération , la perte ou même la duplication de trames.

Le rôle d'un protocole de liaison : est de masquer les défauts du support de transmission afin d'assurer un transfert des données avec un taux d'erreurs négligeables.

On distingue deux méthodes de protection contre les erreurs:

- 1- les méthodes de protection pour la détection.
- 2- Les méthodes de protection pour la correction.

4-4-1-les méthodes pour la détection:

pour ce type de protection l'information de redondance doit être déterminée de manière telle que le récepteur puisse seulement détecter les erreurs de transmission, la correction se fera dans une seconde phase, par le biais de technique de retransmission.

1-1 : la parité transversale :

l'information est dans ce cas formée d'un seul bit de parité ajouté à chaque caractère c-à-d une séquence n bits devient une séquence de (n+1)bits exp : la transmission asynchrone, les protocoles synchrone basé caractères utilisés généralement dans le cas où la probabilité d'erreurs est jugée faible.

1	0	1	1	1	1	0	Parité=1
---	---	---	---	---	---	---	----------

Il y a deux types de parité :

- ❖ **La parité paire** : le nombre total des bits égaux à 1 dans la séquence émise est paire.
- ❖ **La parité impaire** : le nombre total des bits égaux à 1 dans la séquence émise est impaire.

1-2 : la parité transversale et longitudinale :

la méthode consiste à protéger chaque caractère par une parité transversale, mais également à protéger chaque colonne au niveau de la trame par une parité longitudinale.

							Parité transversale
Parité	Longitudinal						
e							

La parité longitudinale est envoyée comme un caractère à la fin de la trame c'est le cas du protocole BSC d'IBM → (BCC: block check character) est un bloc de parité longitudinale.

L'inconvénient de cette méthode de protection est qu'elle est inefficace en cas d'occurrence d'erreurs groupées

1-3 les codes polynomiaux (CRC : le code redondant cyclique):

L'utilisation des codes polynomiaux permet de calculer pour chaque séquence de données utiles une séquence de données redondantes garantissant une protection relativement efficace contre les erreurs groupées, utilisée généralement par les protocoles orientés bit. (BOP) par exemple l'HDLC.

Soit : $i_1i_2i_3\dots i_m$: une séquence de données utiles, et $r_1r_2r_3\dots r_k$: une séquence de données redondantes

On définit deux polynômes :

$$I(x) = i_1x^{m-1} + i_2x^{m-2} + i_3x^{m-3} + \dots + i_{m-1}x + i_m$$

$$R(x) = r_1x^{k-1} + r_2x^{k-2} + r_3x^{k-3} + \dots + r_{k-1}x + r_k$$

Soit un polynôme générateur : $G(x)$ de degré k .

Tel que $R(x)$ = le reste de la division de $I(x)x^k$ par $G(x)$, en d'autres termes :

$$I(x)x^k + R(x) = Q(x) * G(x), \text{ tel que } Q(x) \text{ est le quotient de la division}$$

Si la transmission est passée sans erreurs la trame reçue est supposée correspondre $I(x)x^k + R(x)$ qui est divisible par $G(x)$ c'est-à-dire que $R'(x) = 0$.

Le champ FCS du protocole HDLC = $R(x)$, et le polynôme générateur utilisé par l'HDLC est

$$G(x) = x^{16} + x^{12} + x^3 + 1$$

À la réception, on divise le polynôme $I(x)x^k + R(x)$ correspondant à la suite totale de bits reçus (information+CRC) par le polynôme générateur. Si le reste calculé est non nul, c'est qu'une erreur s'est produite dans la transmission. Si le reste est nul, on est à peu près sûr (99,975% avec le polynôme générateur $G(x) = x^{16} + x^{12} + x^3 + 1$ de la norme V41 du ITU-T) que la transmission s'est faite sans erreur.

Pourquoi cela fonctionne-t-il? Il est évident que $x^k * I(x) + R(x)$ est divisible par $G(x)$, mais en arithmétique modulo 2 addition et soustraction sont équivalentes (ce sont des OU exclusifs en fait) donc on a également $E(x) = x^r I(x) + R(x) = G(x)Q(x)$ montrant que E est un polynôme multiple de G .

il faut aussi remarquer un inconvénient de cette méthode qui signale des erreurs de transmission même si celles-ci ont eu lieu dans le CRC et non dans l'information à transmettre initialement. Dans ce cas il ne devrait pas être nécessaire de retransmettre l'information, or c'est ce qui est fait puisque globalement le transfert (info+CRC) a subi des perturbations. si $E(x)$ le polynôme formé par les erreurs est divisible par $G(x)$ alors le reste =0 et l'erreur est indétectable.

Enfin , comme avantages:Il permet la détection des erreurs groupées formées de k bits.

4-4-2-Méthodes de protection pour la correction :

Pour ce type de protection l'information redondante doit être déterminée de manière telle que le récepteur puisse non seulement détecter les erreurs mais également procéder à leur correction la solution la plus simple consiste à émettre chaque information en plusieurs exemplaires (trop coûteuse).

Par exemple, le code de Hamming est un code correcteur d'erreurs basé sur la notion de distance de Hamming.

Soit un alphabet composé de 4 caractères (00,01,10,11). Si une erreur se produit alors le caractère émis est transformé en un autre caractère et il n'y a pas moyen de retrouver le caractère original.

Par contre, en ajoutant de l'information de telle sorte que les caractères soient très différents les uns des autres cela devient possible. Par exemple, on peut coder les 4 caractères de la manière suivante

caractère initial	00	01	10	11
caractère émis	00000	01111	10110	11001
erronées	00001	01110	10111	11000
	00010	01011	10100	11011
	00100	00111	10010	11101
	10000	11111	11110	10001

Tab. 1.1 - Codage de Hamming.

illustrée dans la table 1.1. Ainsi si un bit (parmi les 5 émis) est erroné on sait quand même déterminer quel caractère a été émis, car comme on peut le voir dans la table 1.1 la modification d'un bit ne peut pas faire passer d'un caractère initial à l'autre. On a des ensembles d'erreurs possibles totalement disjoints. Par contre la modification de 2 bits dans cet exemple peut amener à des confusions et à l'impossibilité de corriger les erreurs. Soit x et y deux caractères d'un alphabet A et soit N la longueur du codage des mots de cet alphabet, x_i et y_i désignent respectivement le i ème bit de x et y . On peut alors définir la distance $d(x; y) = \sum_{i=1}^N (x_i - y_i) \bmod 2$ qui permet de compter le nombre de bits qui diffèrent entre x et y . On définit alors la distance de Hamming par $d_H = \inf d(x; y)$

Ainsi, quand on reçoit un caractère x (erroné ou non on ne peut pas le savoir à l'avance) il suffit de chercher le caractère $c \in A$ le plus proche de x selon la distance d pour obtenir le caractère émis.

Un exemple de code de Hamming est donné par la technique suivante où l'on veut envoyer des caractères codés sur 4 bits de données ABCD. Pour cela on va émettre la suite ABCP3DP2P1

ajoutant une suite de trois bits de données redondantes P1P2P3 tel que les bits de contrôle P_i sont placés sur les bits de rang 2^i et son définis par de manière à satisfaire le système d'équation (ensemble d'équations) tel que

$$P1=A+C+D$$

$$P2=A+B+D$$

$$P3=A+B+C$$

Les P_i sont les bits de parité à l'aide des bits de parité de rang K tel que la décomposition de k en somme de puissance de 2 contient 2^i

A la réception , le récepteur calcule les équations suivantes :

$$P'1=P1+A+C+D$$

$$P'2=P2+A+B+D$$

$$P'3=P3+A+B+C$$

Si on obtient $P'3=P'2=P'1=0$ alors c'est que la transmission s'est passée sans problème , sinon la valeur binaire $P'3P'2P'1$ donne la place de l'erreur dans les bits reçus (on commençant par la droite)on corrige alors l'erreur et

on recalcule les P_i s'ils sont devenus tous nuls l'erreur a été corrigée , sino il y avait eu au loin deux erreurs alors l'émetteur doit retransmettre à nouveau cette trame.

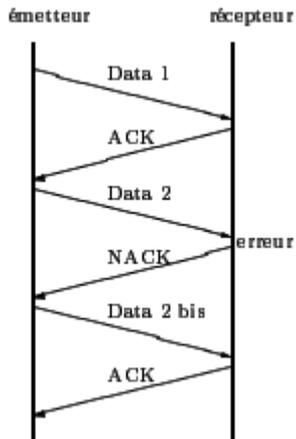
4-4-3 Méthodes de correction par retransmission :

Ces méthodes sont appelées méthodes de retransmission automatiques (ARQ automatique repeat request) on distingue trois types :

a/ retransmission avec arrêt et attente (Idle RQ) :

à la réception d'une trame d'information correcte par le receveur , il renvoie à l'émetteur une trame d'acquittement (un accusé de réception) , une trame d'acquittement de taille relativement courte .

Sert à acquitter une ou plusieurs trames.

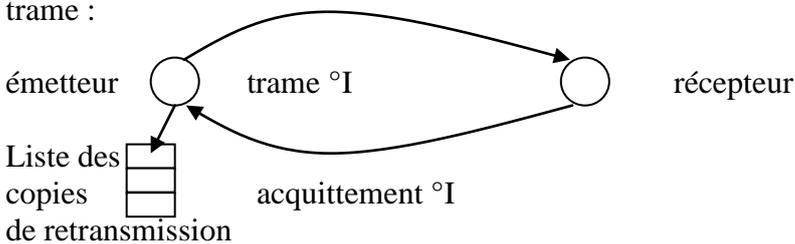


Un délai de garde est armé à l'émission si à l'expiration du délai pas d'acquittement reçu , alors l'émetteur suppose que la trame perdue.

Même en cas de perte d'acquittement , il y aura une retransmission de la trame plusieurs fois, au bout d'un nombre limite de retransmission , la liaison est supposée défectueuse , la couche supérieure est informée.

b/retransmission continue (Continuous RQ)

l'émetteur transmet plusieurs trames d'informations successivement sans attendre d'acquittement pour chaque trame :



on arme une horloge de délai de garde pour chaque trame émise.

On garde une copie des trames émises dans une liste de retransmission.

Les trames et les acquittements sont numérotés.

Si le délai de garde $\neq 0$ et l'acquittement n'est pas reçu $N^{\circ}(i)$.

Retransmission de la trame $N^{\circ}(i)$.

Sinon

Désarmer l'horloge $N^{\circ}(i)$

Retirer la copie de la trame à partir de la liste de retransmission.

Finsi.

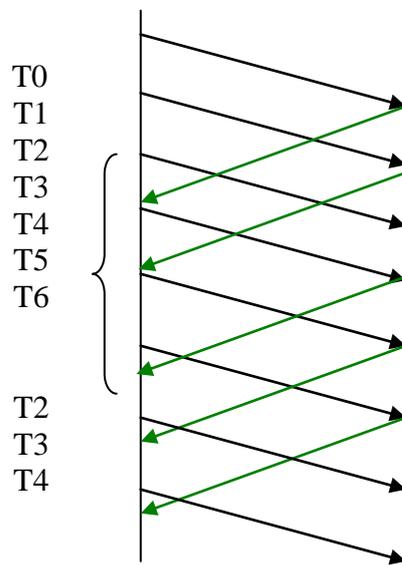
Il y a deux méthodes de retransmission continue :

b-1 retransmission systématique (Go-Back-N) :

le receveur acquitte les trames correctes et qui sont reçues dans l'ordre par exemple : le recepeteur à reçu correctement t2t3t5t6 dans ce cas les trames t5 et t6 seront ignorées.

à l'expiration du délai de garde de la tarme t4 , l'émetteur retransmettra les trames t4 , t5 et t6 .

Le recepeteur n'envoie pas d'acquittement vers l'émetteur que pour les trames reçues dans l'ordre supposons que la trame



On peut améliorer la retransmission systématique par l'utilisation des acquittements positives et négatives.

- Positive (I+1) signifie que I est bien reçue même en cas de perte de l'acquittement de (I).
- Négative(I) signifie que la trame I n'est pas reçue commencer à retransmettre à partir de I.

b-2 retransmission sélective.

Le receveur acquitte les trames correctement reçues même arrivées dans le désordre, il garde une liste de réception où les trames seront réorganisées.

Si une trame t_i n'est pas reçue, mais on reçoit une trame $i+1$ alors le receveur acquitte la trame $i+1$ par un acquittement $i+1$.

A l'expiration du délai de garde et à la réception de l'acquittement de la trame suivante, la trame non acquittée et retransmise elle seule.

Comparaison entre selective et systématique :

- 1-dans systématique : la liste de réception est réduite et ne contienne que la dernière trame reçue.
- 2-l'encombrement du canal par des trames retransmises.

Pour les deux cas on peut si on a une configuration fullduplex, de mélanger une trame d'information du receveur avec l'acquittement attendu, ceci est appelé « Piggybacking ».

5-4-La régulation de flux :

L'objectif du contrôle de flux est d'adapter le débit de l'émetteur en fonction de la capacité d'absorption du récepteur, tout en assurant une utilisation maximale de capacité du canal.

1-mécanisme X-on/X-off (protocole orienté caractère).

Pour les liaisons asynchrones simples

X-on, X-off : sont deux caractères de code ascii

X-off : indique à l'émetteur de cesser toute émission.

X-on : indique à l'émetteur de reprendre son émission.

2-mécanisme de la fenêtre (Protocole orienté bits)

L'idée de fixer le nombre de trames maximum qui peuvent être émises par l'émetteur sans attente d'acquittements, est égale à la taille de la liste de retransmission dès que le nombre est atteint l'émission est stoppée.

L'émission ne peut reprendre que lorsque une ou plusieurs ont été acquittés.

Remarque :

Lorsque le récepteur n'est plus en mesure d'absorber de nouvelles trames, il suffit donc que le récepteur retarde l'envoi d'acquittement l'émetteur et contraindre le dernier à cesser toute nouvelle émission de trames.

- La fenêtre à l'émission : dépend de la taille maximum de trames, le nombre de tampon disponibles, le débit de canal.

- La fenêtre en réception : l'ensemble de trame que l'émetteur est disposé à accepter dépend du type de retransmission implémentée.
- Le cas de la systématique =1.
- Le cas de la retransmission sélective= au moins à la taille de la fenêtre en émission.

Le modulo utilisé :

- 1- en cas de retransmission systématique ($k+1$).
- 2- En cas de retransmission sélective ($2k$).

CHAPITRE 5 : LA COUCHE RÉSEAU

Le rôle de la couche réseau est de transporter des paquets d'un nœud à un autre nœud connecté au même réseau :

Ce niveau 3 (réseaux) réalise trois fonctions principales.

- 1- Le contrôle de flux et l'évitement de congestion.
- 2- Le routage.
- 3- L'adressage.
- 4- Et en plus la détection d'erreur (qui ne sont pas détecter par la couche liaison).

Le contrôle de flux permet l'évitement des congestions dans le réseau.

Le routage : permet d'acheminer les paquets d'informations vers leurs destinations (peut être centralisé ou distribué).

L'adressage : représente l'ensemble des moyens permettant de désigner un élément dans un réseau.

L'adresse IP (utilisateur, processus, autre,...).

Les protocoles de la couche réseau peuvent être classifiés en :

- 1- Mode avec connexion : circuit virtuel (commutation de cellule).
- 2- Mode sans connexion : commutation de paquet datagrammes.

5-1 Le contrôle de flux (de réseau) :

Consiste à gérer les paquets pour qu'ils transitent le plus rapidement possible entre l'émetteur et le récepteur, il cherche à éviter les problèmes de congestion du réseau qui surviennent lorsque trop de message circulent dedans, on peut citer quelques méthodes :

- **Le contrôle par crédit** : seuls N paquets sont autorisés à circuler simultanément sur le réseau, donc un paquet ne peut entrer dans le réseau qu'après avoir acquis un jeton qu'il relâche lorsqu'il arrive à destination.
- **Le contrôle par jeton dédié** : cette technique améliore la précédente en imposant au jeton de retourner à l'émetteur et à l'émetteur de gérer une file d'attente des paquets émis.
- **Le mécanisme de la fenêtre** : dans le cadre d'un circuit virtuel établi entre l'émetteur et le récepteur, les paquets sont numérotés modulo 8 et contiennent que deux compteurs P(s) et P(r), l'émetteur n'est autorisé à émettre que les paquets inclus dans la fenêtre w, tel que l'inégalité suivante soit vérifiée. $\boxed{\text{dernier}(r) \text{ reçu} \leq P(s) \text{ courant} \leq \text{dernier}(r) \text{ reçu} + W}$.

5-2 Résoudre le problème de la congestion :

La congestion est le phénomène de surcharge d'un ou de plusieurs nœuds de commutation se traduisant par une dégradation des performances, voir écoulement de réseau.

Ce phénomène apparaît lorsque le trafic d'entrée dépasse la capacité d'écoulement et s'accroît avec le temps.

Malgré tous les efforts pour contrôler le flux d'information d'un réseau celui-ci peut se retrouver face à un problème de congestion. Il s'agit alors de résoudre le problème sans l'aggraver, en effet les problèmes de congestion arrivent lorsque les files d'attente d'un nœud réseau se trouvent saturées, et donc perdent des paquets.

Un nœud congestionné n'est pas en mesure d'accepter de nouveau paquet, ce qui va conduire à la surcharge des nœuds voisins.

Solution :

- 1- **Contrôle par pré-allocation de tampons** : uniquement en cas de circuit virtuel (réserver à l'avance des tampons pour chaque circuit virtuel, ce qui permettra de régler le flux).

Résout le problème, mais il sous-utilise la liaison.

- 2- **Contrôle basé sur l'écartement des paquets** : (rejeter les paquets reçus lorsque les tampons sont pleins, mais avant de rejeter il faut vérifier la nature des paquets, parce que si c'est un acquittement, cela peut libérer des tampons pleins. Cette technique conduit à une mauvaise utilisation de la liaison.
- 3- **Contrôle basé sur signal de ralentissement** : (chaque nœud surveille ses propres files d'attente d'entrée, on part de l'observation qu'une ligne de sortie entre dans un état critique lorsque elle atteint un certain pourcentage (ex : 70%).
- 4- **Le contrôle par durée de péremption** : on n'autorisant un paquet de rester dans le réseau qu'un temps limité, tout paquet est donc émis avec une date fixée par une horloge commune au réseau, si un nœud s'aperçoit que le temps de présence dans le réseau d'un paquet est dépassé il le détruit, pour simplifier l'implémentation un compteur au lieu de la date est sauvegarder dans le paquet, à chaque passage par un nœud de commutation il est décrémenté, quand sa valeur sera zéro, le nœuds, qu'il le reçoit va le détruire.

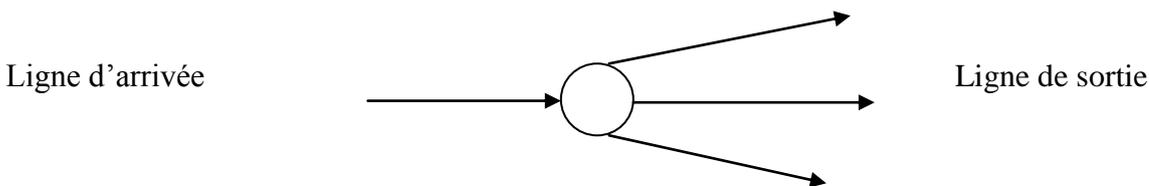
5-3 Introduction aux algorithmes de routage

Le rôle d'un algorithme de routage est de déterminer le chemin que doit prendre un paquet à l'intérieur d'un réseau de communication pour se rendre d'un nœud source à un nœud destinataire.

L'algorithme est réparti sur tous les nœuds du réseau et permet à chacun d'eux d'aiguiller tout paquet en transit sur la meilleure ligne de sortie.

Le Routage :

Le routage des paquets dans un réseau maillé consiste à fixer par quelle ligne de sortie chaque commutateur réexpédie les paquets qu'il reçoit. ceci se fait en fonction de la destination finale du paquet et selon une table de routage qui indique pour chaque destination finale quelles sont les voies de sortie possible.



2-1. Les désavantages d'un mauvais algorithme de routage :

Les décisions de routage sont prises indépendamment les unes des autres au niveau de chaque nœud. Ce qui pourrait causer certains problèmes, tels que les suivants :

- le paquet peut emprunter des chemins en boucle à l'intérieur du réseau.
- Le paquet peut osciller indéfiniment entre deux nœuds voisins.
- La surcharge par un flux considérable de paquets vers un même nœud peut causer la congestion du réseau.

2-2. Les qualités d'un bon algorithme de routage :

- Choisir le chemin le plus court ou le plus économique.
- Eviter de router des paquets vers un nœud déjà congestionné.
- Eviter de renvoyer les paquets sur la ligne par laquelle ils sont parvenus au nœud.

2-3. Classification des algorithmes de routage :

1-Algorithmes de routage fixe :

Un algorithme de routage fixe est un algorithme qui permet d'associer à tout couple de nœuds source et destination un chemin déterminé de manière statique. Pour réaliser cette technique on utilise une table de routage fixe.

Avantages : simplicité de l'implantation.

Inconvénients : non adaptée pour le trafic variable ; insensible au défaillance de réseau (congestion, panne).

destination	Sortie
D1	L1
D2	L2
D3	L5

2-Algorithmes de routage adaptatif centralisé :

Un algorithme de routage adaptatif centralisé est basé sur la coopération entre un nœud particulier, appelé « centre de contrôle du routage » et les autres nœuds du réseau qui entretiennent des tables de routages locales.

Le fonctionnement :

Tous les nœuds envoient périodiquement des comptes rendus au serveur pour estimer puis envoyer à chaque nœuds les changements nécessaires sur leurs tables locales.

Avantages : mieux adaptés au trafic variable.

Inconvénients :

- le transit de comptes-rendus engendre un trafic supplémentaire pouvant causer la congestion.
- Les modifications des tables envoyées par le centre peuvent être périmées (changement de l'état du réseau).
- L'intolérance aux problèmes de pannes du centre.

3-Algorithmes de routage adaptatif réparti.

Dans cette technique aucun nœud ne joue le rôle d'un centre de contrôle.

Fonctionnement :

Chaque nœud met à jour sa table de routage en exploitant des informations locales parvenant des nœuds voisins (état et délais).

5-4 L'adressage :

Toutes les machines sur l'Internet sont identifiées grâce à une suite de chiffres: **l'adresse IP**.

5-4-1 Qu'est-ce qu'une adresse IP ?

Sur l'Internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx.

Par exemple, 194.153.205.26 est une adresse IP.

Ces adresses servent aux ordinateurs du réseau pour communiquer entre-eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

C'est l'Icann (Internet Corporation for Assigned Names and Numbers, remplaçant l'IANA (Internet Assigned Numbers Agency) depuis 1998, qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public Internet.

5-4-2 Déchiffrement d'une adresse IP

Une adresse IP est une adresse 32 bits, généralement notée sous forme de 4 nombres entiers séparés par des points. On distingue en fait deux parties dans l'adresse IP:

- 1- Une partie des nombres à gauche désigne le réseau est appelée ID de réseau (en anglais netID),
- 2- les nombres de droite désignent les ordinateurs de ce réseau est appelée ID d'hôte (en anglais, host-ID).

Imaginons un réseau noté 58.0.0.0. Les ordinateurs de ce réseau pourront avoir les adresses IP allant de 58.0.0.1 à 58.255.255.254. Il s'agit donc d'attribuer les numéros de telle façon qu'il y ait une organisation dans la hiérarchie des ordinateurs et des serveurs.

Ainsi, plus le nombre de bits réservé au réseau est petit, plus celui-ci peut contenir d'ordinateurs.

En effet, un réseau noté 102.0.0.0 peut contenir des ordinateurs dont l'adresse IP peut varier entre 102.0.0.1 et 102.255.255.254 ($256*256*256-2=16777214$ possibilités), tandis qu'un réseau noté 194.26 ne pourra contenir que des ordinateurs dont l'adresse IP sera comprise entre 194.26.0.1 et 194.26.255.254 ($256*256-2=65534$ possibilités), c'est la notion de classe d'adresse IP.

5-4-3 Adresses particulières

1- Lorsque l'on annule la partie host-id, c'est-à-dire lorsque l'on remplace les bits réservés aux machines du réseau par des zéros (par exemple 194.28.12.0), on obtient ce que l'on appelle l'adresse réseau. Cette adresse ne peut être attribuée aucun des ordinateurs du réseau.

2- Lorsque la partie netid est annulée, c'est-à-dire lorsque les bits réservés au réseau sont remplacés par des zéros, on obtient l'adresse machine. Cette adresse représente la machine spécifiée par le host-ID qui se trouve sur le réseau courant.

3- Lorsque tous les bits de la partie host-id sont à 1, l'adresse obtenue est appelée l'adresse de diffusion (en anglais broadcast). Il s'agit d'une adresse spécifique, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le netID.

4- A l'inverse, lorsque tous les bits de la partie netid sont à 1, l'adresse obtenue constitue l'adresse de diffusion limitée (multicast).

5- Enfin, l'adresse 127.0.0.1 est appelée adresse de rebouclage (en anglais loopback), car elle désigne la machine locale (en anglais localhost).

5-4-4 Les classes de réseaux

Les adresses IP sont réparties en classes, selon le nombre d'octets qui représentent le réseau.

Classe A

Dans une adresse IP de classe A, le premier octet représente le réseau.

Les réseaux disponibles en classe A sont donc les réseaux allant de 1.0.0.0 à 126.0.0.0 (les derniers octets sont des zéros ce qui indique qu'il s'agit bien de réseaux et non d'ordinateurs !)

Classe B

Dans une adresse IP de classe B, les deux premiers octets représentent le réseau.

Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 2^{14} (10 000000 00000001 à 10 111111 11111110) possibilités de réseaux, soit 16382 réseaux possibles. Les réseaux disponibles en classe B sont donc les réseaux allant de 128.1.0.0 à 191.254.0.0

Classe C

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1, 1 et 0, ce qui signifie qu'il y a 2^{21} - 2 possibilités de réseaux, c'est-à-dire 2097150. Les réseaux disponibles en classe C sont donc les réseaux allant de 192.0.0.0 à 223.255.254.0

L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir:

$2^8 - 2^1 = 254$ ordinateurs.

5-4-5 Attribution des adresses IP

Le but de la division des adresses IP en trois classes A, B et C est de faciliter la recherche d'un ordinateur sur le réseau. En effet avec cette notation il est possible de rechercher dans un premier temps le réseau que l'on désire atteindre puis de chercher un ordinateur sur celui-ci. Ainsi l'attribution des adresses IP se fait selon la taille du réseau.

Les adresses de classe A sont réservées aux très grands réseaux, tandis que l'on attribuera les adresses de classe C à des petits réseaux d'entreprise par exemple

5-4-6 Adresses IP réservées

Il arrive fréquemment dans une entreprise ou une organisation qu'un seul ordinateur soit relié à internet, c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à internet (on parle généralement de proxy ou de passerelle).

Dans ce cas de figure, seul l'ordinateur relié à internet a besoin de réserver une adresse IP auprès de l'Icann. Toutefois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble en interne.

Ainsi, l'Icann a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet sans risquer de créer des conflits d'adresses IP sur le réseau des réseaux.

- Adresses IP privées de classe A : 10.0.0.1 à 10.255.255.254, permettant la création de vastes réseaux privés comprenant des milliers d'ordinateurs.
- Adresses IP privées de classe B : 172.16.0.1 à 172.31.255.254, permettant de créer des réseaux privés de taille moyenne.
- Adresses IP privées de classe C : 192.168.0.1 à 192.168.255.254, pour la mise en place de petits réseaux privés.

5-4-7 Format d'un paquet IP :

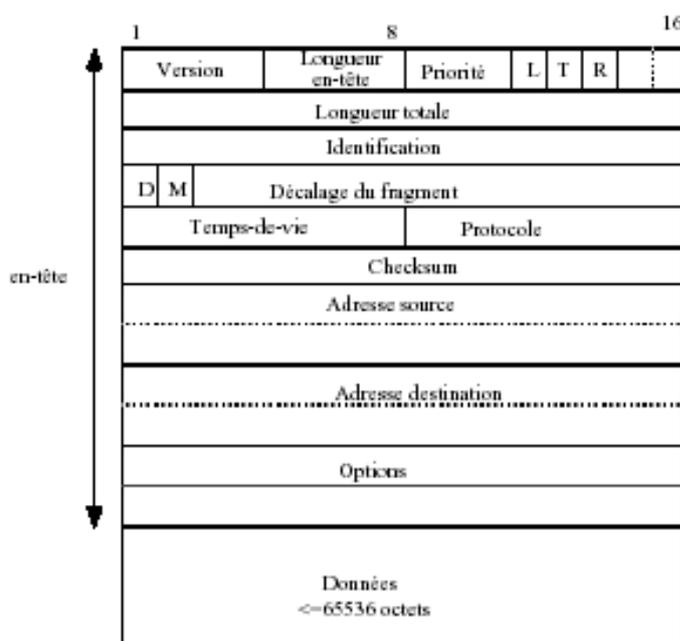
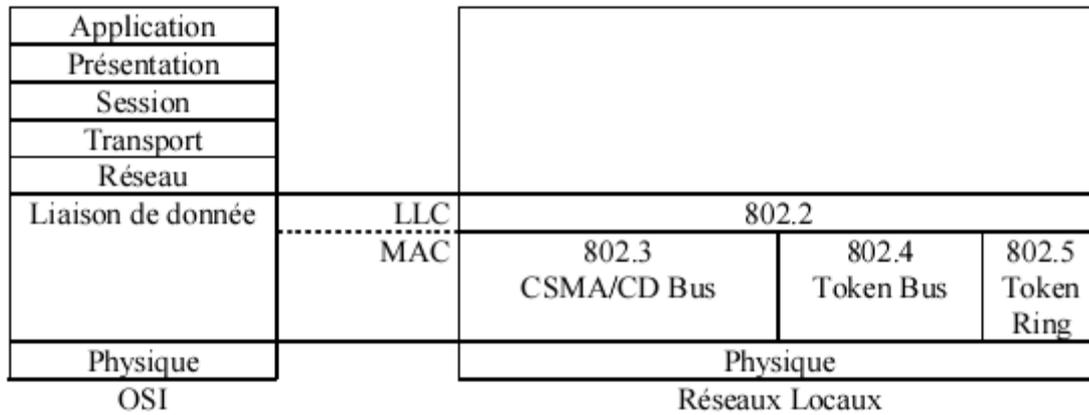


Figure 1. Format d'un paquet IP.

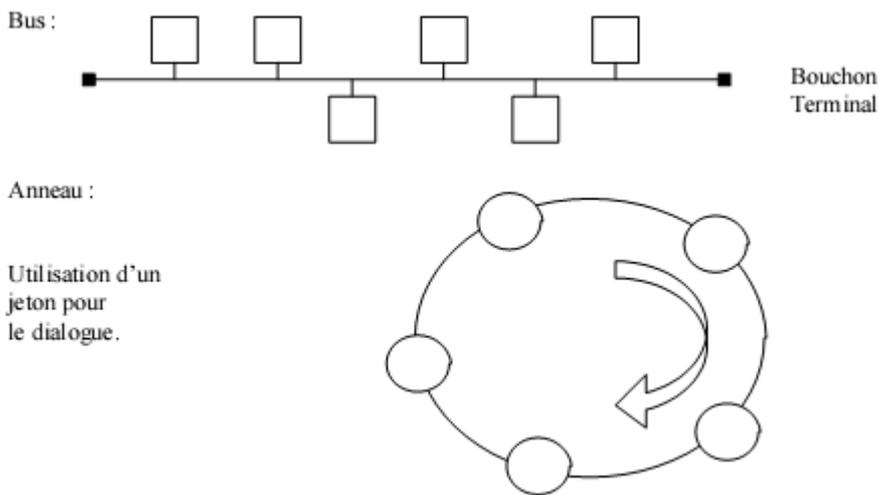
- La version est 4 ce qui signifie un adressage à 4 octets. La version IPv6 sera sur 6 octets.
- Les champs priorité et type de service permettent d'accélérer les transactions en choisissant éventuellement le meilleur support.
- Chaque paquet IP reçoit une identification construite par le service qui l'utilise.
- Les paquets sont donc en général fragmentés et le décalage des fragments est donc contenu dans un paquet IP.
- Le temps de vie est décrémenté de 1 à chaque passage dans un routeur.
- Le checksum est un calcul effectuée sur l'ensemble du paquet pour garantir son intégrité.
- Le champ protocole identifie le protocole qui a fourni le paquet à IP (UDP, TCP,...).
- Le paquet contient les numéros des hôtes source et destination.

- Les options comportent des possibilités qui ne sont pas supportées par tous les routeurs. Il s'agit de :
 - sécurité,
 - enregistrement de la route suivie,
 - estampillage horaire,
 - routage peu strict de la source,
 - routage strict de la source.

CHAPITRE 6 : LES RESEAUX LOCAUX



Topologie de réseaux locaux



Niveau 2 des réseaux locaux

Dans les réseaux locaux, on utilise des procédures un peu différentes de HDLC principalement parce qu'il est nécessaire d'assurer en plus des fonctions d'accès au support. Les techniques utilisées restent similaire à celle HDLC.

La couche liaison de donnée des réseaux locaux est divisée en deux sous – couches.

- La sous – couche LLC (Logical Link Control)
- La sous – couche MAC (Medium Access Control)

La sous – couche MAC à fait l'objet de trois normes :

802.3 : Réseau en bus CSMA/CD

802.4 : Token bus

802.5 : Token ring

c) La norme 802.3 ou CSMA/CD

- Principe :

CSMA/CD est une technique basée sur le principe d'écoute, de compétition et de détection de collision.

CSMA/CD : Carrier Sens Multiple Access / Collision Detected.

- Algorithme :

Le principe d'accès au support est la compétition : un émetteur utilise la voie dès qu'il est prêt à émettre.

Il ignore donc les autres émetteurs.

Risque de collision.

Pour limiter le nombre de collision, cette technique utilise le principe d'écoute : un émetteur n'émette que s'il n'y a pas de transmission en cours.

d) La norme 802.4 : Token Bus

- Topologie physique du réseau, c'est le bus.
- Topologie logique : Anneau.

L'allocation du bus est déterminée par la circulation d'un jeton (droit d'émission). Cette technique a été retenue car elle assure un délai borné pour l'accès au bus.

Les types de réseaux locaux

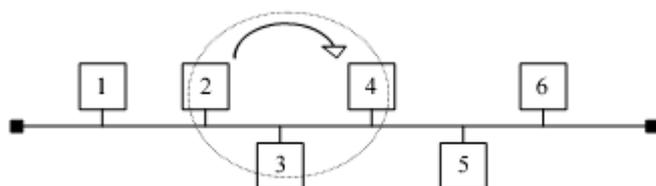
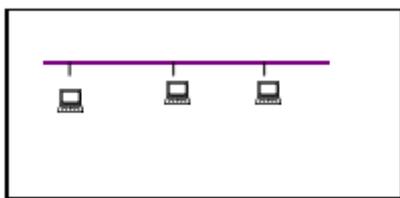
Le But :

Raccorder sur un même support physique des ordinateurs, et permettre de communiquer avec un ensemble d'ordinateurs sur ce support. Un seul message sur le support peut être lu par plusieurs ordinateurs. Les modems sont remplacés par des cartes réseaux que l'on installe dans les ordinateurs. Ces réseaux sont de taille limitée. Cette limite est due au protocole lui-même.

On trouve schématiquement deux types de réseaux, les BUS et les Anneaux

Dans le cas des BUS, tout le monde parle sur un même fil. Pour gérer les collisions inévitables, on s'empare du fil en émettant suffisamment longtemps (le temps de la propagation aller/retour du signal sur le support), pour s'assurer que le message a été correctement lu.

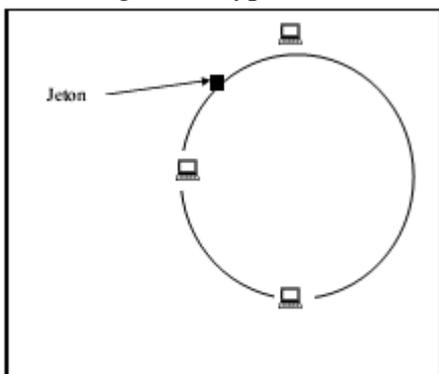
ETHERNET est de type BUS



Anneau virtuel : elles vont parler à tour de rôle.

Dans le cas des Anneaux, une trame vide circule en permanence sur le fil qui relie l'ensemble des machines. Cette trame s'appelle le jeton. La machine qui a le jeton peut y insérer des données. Le jeton peut être perdu. Le temps de réaction à cette perte encadre la dimension du réseau et le nombre des machines qui peuvent s'y connecter. Les anneaux se comportent mieux sous forte charge.

Token Ring est de type Anneau à Jeton



ETHERNET ou le début du réseau Local (RFC 894 et 1042)

ETHERNET a été développé par Xerox Corporation au Palo Alto Center (PARC) vers le milieu des années 70. Il fut suite au développement d'un projet de réseau (ALOA) de l'Université de Hawaii. A cette époque, le concept de réseau local n'existe pas, le micro-ordinateur non plus. Bref un peu de paléontologie..

ETHERNET est novateur car la vitesse d'échange entre ordinateurs n'excédait guère 64 Kilo bits par seconde. Le principe est donc de mettre un support physique en commun, et de faire du très haut débit sur des distances moyennes (>100m).

La spécification de ETHERNET a été faite conjointement par DEC, Xerox et Intel.

On utilise un câble commun pour relier des dizaines voire des centaines de machines. Ce câble commun va véhiculer les informations à destination de l'ensemble des stations, la méthode utilisée est le CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

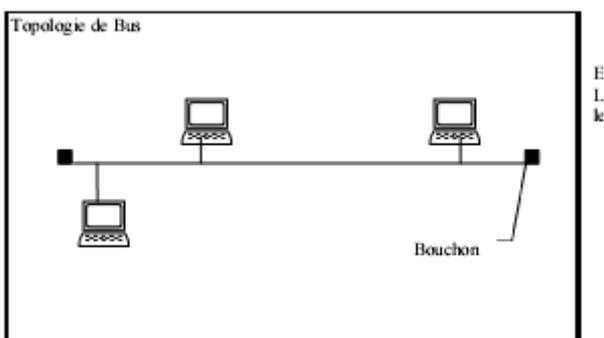
Le Câble forme un BUS dans le jargon réseau, reliant les stations. La vitesse est fixée par la norme : 10 Mbs. (10 Millions de bits par seconde). Un bit est une valeur binaire : 0 ou 1.

La notation IEEE802.3 :

10Base5 10=10Mbs Base=Bande de Base 5 = 5*100mètres ex

Nom	10 Base 5	10 base2	1 Base5	10BaseT (1985)	10Broad 36
Vitesse Mbps	10	10	1	10	10
Signal	Baseband	Baseband	Baseband	Baseband	Broadband
Longueur Max	500	185	250	100	1800
Media	50 Ohm coax (thick)	50 Ohm coax (thin)	Unshielded Twisted Pair	UTP	75 ohm coax
Topologie	Bus	Bus	Bus	Etoile	Bus

Un certain nombre de réseaux cités sont très rares (10Broad36 ou 1Base5).



Problème : Comment parler sans que ce soit le désordre ? ETHERNET a dû répondre à ce problème Ce protocole est aléatoire, chacun parle quand il a envie, mais suivant des règles strictes. Si deux machines émettent en simultanément, il se produit une collision. Celle-ci n'est détectée que pendant l'émission d'une trame.

1. Avant de parler on écoute le câble. Si silence étape 2.
2. On émet une trame de 64 octets minimum et au plus 1518 octets. La collision doit être détectée pendant l'émission de la plus petite trame. Celle-ci comprend 64 octets, soit 512 bits transmis en 51,2 μ s (à 10 Mbit/s). On écoute pendant l'émission, il faut avoir le retour d'information comme quoi une collision vient d'arriver. Pour cela la longueur maximum du réseau correspond à une durée de 25,6 μ s. Si l'on 5 -6 = utilise une fibre optique, la longueur maximum en km sera de $3 \cdot 10^8 \cdot 25,6 \cdot 10^{-6}$ 7km. En fait ce cas est rare car la vitesse est plus faible dans les câbles, de plus le signal s'affaiblit et il faut le régénérer par des répéteurs qui ont des temps de traversée. C'est souvent plus proche de 500m.
3. Le signal se propage comme une onde qui va parcourir le câble. Or, des stations ont pu croire que la câble était libre et se mettent à parler. Il se produit dans le jargon ETHERNET, une collision. On détecte une trame brouillée (Jam).

4. Si collision, on émet une trame de brouillage, on calcule un nombre aléatoire et on attend avant de réémettre . Toutes les stations font le même calcul. Passé ce délai, on réémet la trame. Et ainsi de suite jusqu'à 16 fois, avant de remonter une anomalie à la couche supérieure.

Le support d'origine était un câble coaxial qui ne comporte qu'un fil central et un blindage. Ce type de support ne permet pas une transmission bidirectionnelle mais juste unidirectionnelle. On dit que la transmission est half-duplex. (on émet ou on reçoit). Ceci a changé avec l'apparition de 10 Base T qui comprend 2 paires de fils, une pour émettre et une pour recevoir. Ceci dit, à part dans les commutateurs ETHERNET modernes le protocole reste half-duplex.

Au delà de la limite de distance du support , on peut étendre le réseau à l'aide de répéteurs qui vont réamplifier le signal vers un autre segment ETHERNET. On ne peut pas traverser plus de 2 à 3 répéteurs.

Au-delà on utilise des ponts . Le pont lit les trames et les réémet, de plus il apprend les adresses ETHERNET et fait office de filtre. Les répéteurs amplifient tout, même les bruits. Le pont travaille au niveau logique, fait du contrôle d'adresses et d'erreurs.

Les ponts peuvent boucler le réseau à condition d'utiliser l'algorithme Spanning Tree. L'expérience montre que loin de faire une redondance entre ponts, la détection des problèmes s'avère fort délicate. Il vaut mieux éviter de boucler un réseau ETHERNET.

Le Format des trames.

On trouve plusieurs formats : IEEE802.3, IEEE802.2, ETHERNET2, ETHERNET SNAP. Pour simplifier, on ne présente que ETHERNET2. TCP/IP utilise la plupart du temps le format ETHERNET2. Pour IEEE802.3 le champ type devient un champ longueur. On ajoute parfois un en-tête dans la partie donnée qui s'appelle le LLC suivi éventuellement du SNAP. Ces en-têtes supplémentaires provoquent une perte de données utiles que TCP/IP évite en prenant le format originel de ETHERNET (II).

Les chiffres indiquent le nombre d'octets (8 bits)

7	1	6	6	2	46-1500	4
Préambule	S O F	Adresse de Destination	Adresse Source	Type	Données	FCS

Préambule :

Attention, une trame arrive, synchronisez vous (Toutes les horloges ont des dérives 10Mb/s +-)

SOF (Start of Frame) Fanion de début de trame (séquence caractéristique).

Source :

Chaque carte a une adresse unique générée par le constructeur de la carte.

Destination :

Soit l'adresse d'une carte, soit une adresse de diffusion de groupe ou de réseau (Broadcast)

Type :

Quel service réseau va lire la trame. Par exemple IP ou NOVELL ou LAN Manager . Ces types sont normalisés. Le type indique à quel logiciel (couche) on va renvoyer les données.

FCS (CRC Cyclic Redundancy Check)

Il existe de toute façon un temps inter trame égal à 12 octets soit 9.6 µsec

TOKEN RING

ou IEEE802.5 ou Anneau à Jeton

Token Ring est le protocole promu par IBM pour se démarquer de ETHERNET. Stratégie industrielle ?, ou vision différente du réseau et de la société. On a vu avec ETHERNET que l'organisation est très anarchiste.

Tout le monde cause quand il veut. Bref IBM n'a pas dû aimer et a inventé l'anneau à jeton . Un jeton tourne, va de station en station. Le jeton est une trame qui circule de station en station. Si vous l'avez et qu'il est vide, vous pouvez y ajouter vos données. Quand on émet, le récepteur prend l'information , indique dans l'en-tête qu'il a lu les données , le récepteur vérifie cette lecture et rend le jeton vide. Cette norme a évolué en vitesse.

Au départ , c'était 4Mb/s, maintenant c'est 16 Mbs. La vérification de la lecture à 16Mb/s n'est pas faite.

Ce protocole était assez novateur pour le câblage, car il utilise du matériel actif équivalent au Hub ETHERNET, ceci bien avant 10BaseT. Avantage aussi, sous forte charge, le réseau ne s'écroule pas, tout le monde a le même temps de parole. Par contre sous faible charge il est plus lent. Les trames sont plus longues. On peut insérer des stations ou des MAU (MAU= medium access unit) à chaud. Les MAU sont alimentées par les stations. Donc

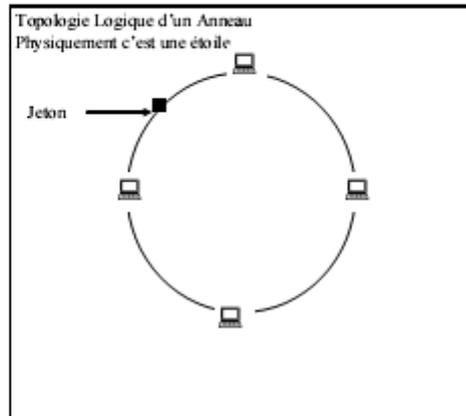
le matériel est très fiable. Un anneau peut compter 256 stations. La vitesse d'émission était de 4Mbs à l'origine, puis 16Mbs ensuite.

Le concept de l'anneau reste d'actualité dans les hauts débits (FDDI)

Format de la trame :

1	1	1	6	6	>=0	4	1
Start Delimiter	Access Control	Frame control	Adresse Destination	Adresse Source	Données	FCS	End Delimiter

Le token = StartDelimiter+AccessControl+EndDelimiter



Une station est le moniteur actif (la première connectée) et contrôle le réseau. Si une station est en panne, une trame peut ne pas s'arrêter .

FDDI ou Fiber Distributed Data Interface

Né au milieu des années 80 : Principe : 100 Mbps, double anneau à jeton utilisant un support fibre optique. Les fibres peuvent être Multimode ou monomode. La différence entre les deux vient du fait que l'une est à gradient d'indice alors que l'autre a un cœur d'un autre indice dont le diamètre est égal à la longueur d'onde de la lumière transportée, celle-ci se propage alors en ligne droite sans dispersion. La monomode est réservée pour des cas particuliers (distance) et ses connecteurs sont chers. On utilise le plus souvent de la multimode dite 62.5/125 µm. Des lasers à diodes semi-conductrices sont utilisés pour émettre, de la même façon que pour la lecture d'un CD-ROM.

La technologie FDDI connaît une nouvelle jeunesse avec l'arrivée des commutateurs FDDI. Ceci dit, elle est très concurrencée par l'arrivée de l'ETHERNET à 100 Mbs et de la commutation ETHERNET à 100Mbs.

On ne lui prédit plus un très grand avenir. Elle existe cependant de nombreux sites qui ont eu des besoins de gros débits avant l'apparition de 100 Base T.

Caractéristiques principales

Distance entre deux nœuds 2kms

2 anneaux contrarotatifs

100 km à plat ou 35 km de diamètre

500 à 1000 stations possibles

Trame maximum de 45000 octets

Tolérance de panne en cas de coupure des anneaux

Pour émettre, il faut avoir le jeton et avoir été accepté par la station de management.

3 compteurs gérés par la station LE TRTT (temps max de rotation du jeton) Le TRT (par rapport au TRTT, combien de temps peut on parler). Si jeton en retard, on n'émet que les informations synchrones (voix, vidéo..)

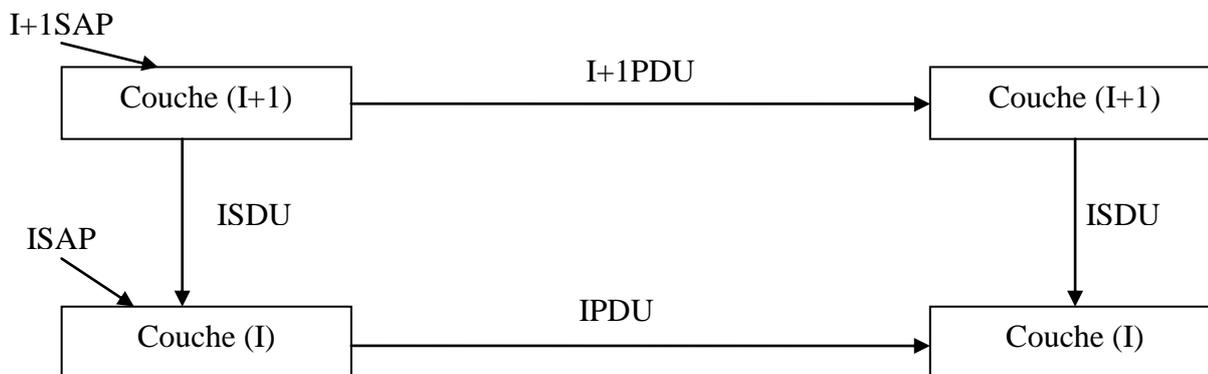
Le THT temps maximal d'émission synchrone (temps réel)

CHAPITRE 7 : PROTOCOLES DE BOUT EN BOUT

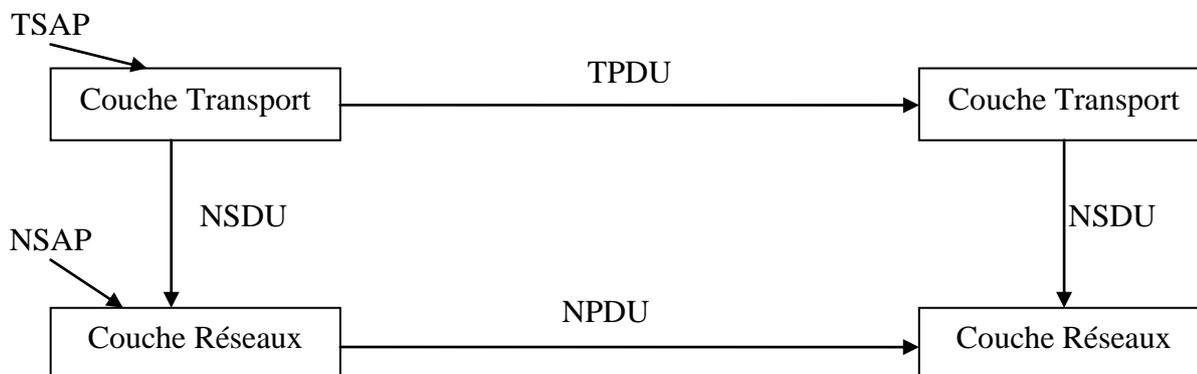
Par protocoles de bout en bout on désigne les protocoles mettant en œuvre uniquement des entités situées au sein de machines hôtes –« protocoles relatifs aux couches transport, session, présentation, et application », exemple –TCP/UDP-.

7.1 Appellations utilisées par l'ISO :

- Données échangées entre deux entités homologues PDU (protocole data unit).
- Données échangées entre deux entités superposées SDU (service data unit).



Le PDU devient SDU quand il est passé vers la couche juste en dessous , par exemple :

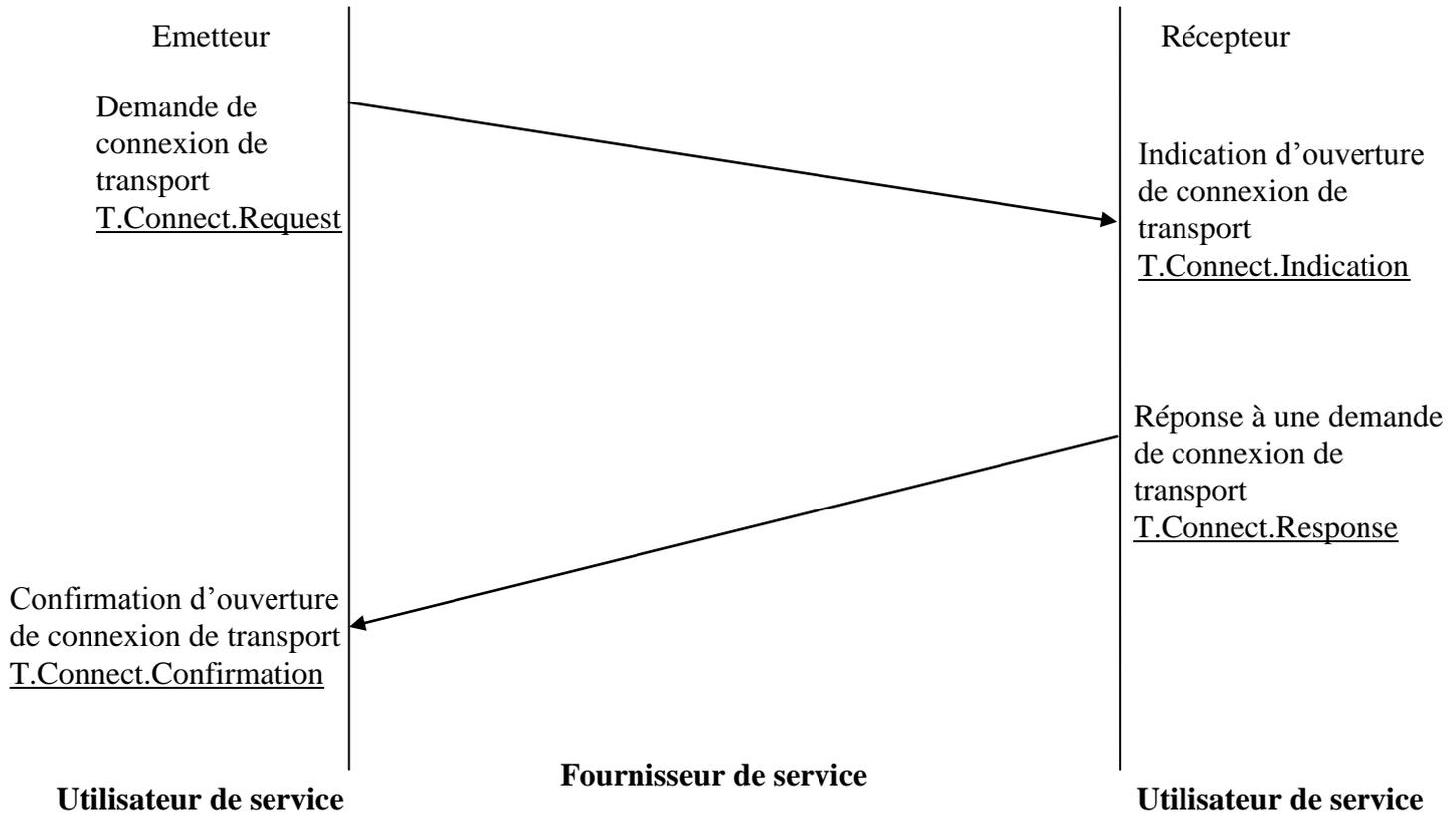


7.2 Le fonctionnement de la couche transport :

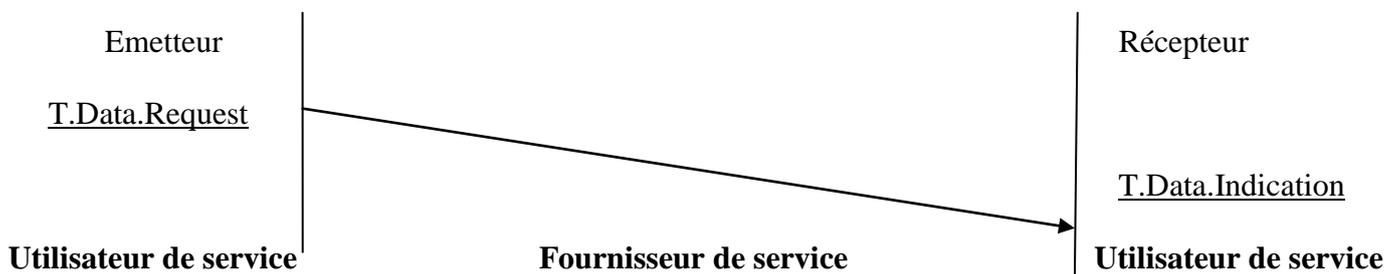
La connexion de transport est mise en œuvre de façon classique par les primitives suivantes :

- Request.
- Indication.
- Response.
- Confirmation.

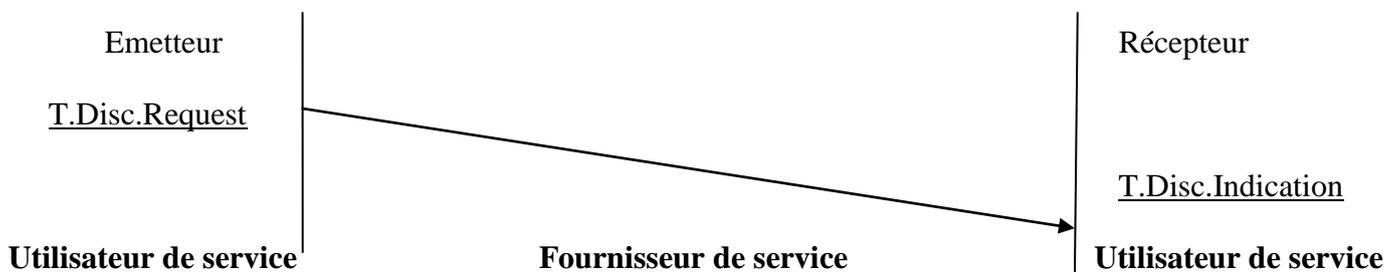
Par exemple pour la phase établissement de connexion :



Par exemple pour la phase échange de données :



Une remarque : les acquittements sont à la charge de la couche réseau
Par exemple pour la phase déconnexion:



7.3 Les services rendus par la couche transport :

1- l'objectif de la couche transport est de rendre complètement indépendantes les fonctions des couches session présentation , application , des caractéristiques du réseau de communication utilisés.

La couche transport fournit ses services soit en mode connecté (exp : le circuit virtuel pour le protocole TCP) ou en mode déconnecté (exp : les datagrammes pour le protocole UDP).

2-le choix de la qualité de service (QoS) :

Cette qualité est négociée entre les utilisateurs et les fournisseurs de services transport (débit de la connexion , temps de transit, taux d'erreur, délai d'établissement de la connexion, probabilité d'échec d'une demande de connexion,débit utile par seconde , temps de transit d'un message dans le réseau, le nombre de paquets perdus par seconde, probabilité qu'un transfert soit erroné, ...).

3- interface entre la couche session et transport :

TSAP numéro de port (N° de socket pour TCP) est l'adresse d'une entité session de destination la taille de TSDU est variable , c-à-d dépend du message , par contre le NSDU ne dépend que de la nature du réseau utilisé (TSDU → fragmenter → 1 ou plusieurs NPDU) , par exemple (21 :FTP, 80 :http,7 :ECHO,23 :TELNET).

4- Le contrôle d'erreur :

Les erreurs telle que la perte ou duplication de paquets se produisant lors de routage entre deux nœuds voisins sont prises en charge par la couche réseau alors que l'erreur au sein de la couche réseau elle-même lors du routage est transparente pour elle.

En utilise généralement N° de séquence ,les acquittements de bout en out, et le CRC , et le délais de garde pour faire face à cette situation.

5- le contrôle de flux :les TSDU ou les messages sont généralement très variables , il n'est pas recommandé de faire une répartition statique des tampons disponibles entre les différentes connexions de transport , il est plus judicieux de mettre en œuvre un mécanisme d'allocation dynamique , attribuant au départ une quantité minimum de tampons à chaque connexion est allouant les reste de la quantité disponible en fonction des besoins . on utilise un mécanisme de fenêtre de taille variable , c-à-d l'acquittement porte la taille de la fenêtre restante .
les octets d'un fragment sont numérotés :

4628 premier octet non acquitté 6676 dernier octet peut être émis 5140 en cours de transmission	5140 prochain octet attendu. 7098 valeur extrême attendue
---	--

7.4 Format d'un fragment de TCP :

16 bits port source	16 bits port destination
N° de séquence	
N° d'acquittement	
Taille d'entête	Taille de fenêtre
Checksum	Pointeur d'urgence
Options	
Données	

Options : (PSH : push fonction délivrer les fragments rapidement., RST : restart transmission)

Pointeur d'urgence : indique le dernier octet d'un message urgent.

En générale pour la couche transport on utilise l'un des deux protocole suivants :

*- le protocole TCP élimine la congestion par un algorithme appelé Slow Start an collision aviodance , son principe de fonctionnement et le suivant : la fenêtre commence avec une taille =1 , et sera doublé suite a chaque acquittement reçu avant l'expiration du délai de garde , si une taille fenêtre donnée cause un retard dans la réception de l'acquittement , alors on remet la fenêtre à 1 et on s'arrête sur N/2 (tel que N : est la taille qui à provoquer le retard).

*- le Protocole UDP : fonctionne en mode sans connexion , et sans reprise sur erreur , et n'utilise aucun acquittement , et ne reséquence pas les messages , et ne met aucun mecanisme de contrôle de flux.

Généralement , ce protocole est utilisé pour les application multimédias (films , son , téléphonie sur internet) parce que il se caractérise par une exécution rapide , appropriée pour les applications temps réels ,....

Port source	Port destination
Longueur	Checksum
Données	

7.5 La couche session :

Cette couche est responsable de l'établissement et le maintien d'une connexion logique (session) entre deux entités de la couche présentation et cela pour la durée d'une transaction.

La pose de points de reprise nécessaires lorsque le réseau tombe en panne et qu'il faut redémarrer sur un point cohérent entre l'émetteur et le récepteur .(par exemple le protocole LU6.2 d'IBM).

L'aspect transactionnel permet d'effectuer plusieurs demande de connexion de courte durée , pour que cela fonctionne la couche session ne doit pas être mise en place puis libérer à chaque demande il existe une ou plusieurs connexion sur lesquelles les conversations sont multiplexées dans le temps ou établir plusieurs connexion transport durant la même session .

En cas de passage par une période d'inactivité la couche session peut libérer la connexion transport.

En générale cette couche réalise les fonctions suivantes :

- 1-gestion de dialogue : fournit un service de communication full ou semi duplex.
- 2-synchronisation de session : au cours d'une session de longue durée la connexion de transport pourrait tomber en panne , la couche permet la définition des points de reprise pour ne pas reprendre du début.
- 3-conversion d'adresse : elle fait la conversion d'adresse locales du processus utilisateur en adresse de transport .

7.6 La couche présentation :

Est responsable de la mise en correspondance des structures et format de données , échangées par les entités correspondantes de la couche application (FTP).

La couche présentation permet à la machine hôtes de garder des représentation internes différentes (EBCDIC,ASCII) , et de transformer ces données en une représentation reconnue par toute les machines connectées lors de la communication avec une autre machine sur le réseau.

Cette représentation est appelée syntaxe commune.

Type abstrait de données ; format virtuel de fichier. (par exemple le protocole ASN1 (abstract syntax notation one).

7.6 La couche application :

Dans cette couche réside les différentes applications réseaux :

- 1- la messagerie électronique.
- 2- Le transfert de fichier .
- 3- Le web.
- 4- La parole téléphonique .
- 5- La vidéo .
- 6- Les autres applications multimédias.

1- la messagerie électronique : cette fonctionnalités est réalisée grâce aux protocole (SMTP : simple mail transfert protocol) elle se servent d'adresse de type student@univ-skikda.dz (compte@domaineserveur) Le format de message est de type ASCII , la récupération du message a partir du serveur se fait par protocole POP (Post Office Protocol) qui travail en mode connecté.

2-le transfert de fichier (utilise le protocole FTP : file transfert protocol) , application client / serveur , cet protocol met en place une session temporaire pour transférer un plusieurs fichiers) qui travail en mode connecté.

3- le WWW (world wide web) , necessite un navigateur dans les bases de données distribuées (IE, FireFox ; Mosila) utilise un protocole http : Hyper text transfert protocol). Travail en mode sans connexion.

4-la parole téléphonique : application complexe demandant un fonctionnement interactif et beaucoup de synchronisation.

Cours Master

Les architectures logiques :

C'est l'empilement de protocoles dédiés à un domaine de communication spécifique.

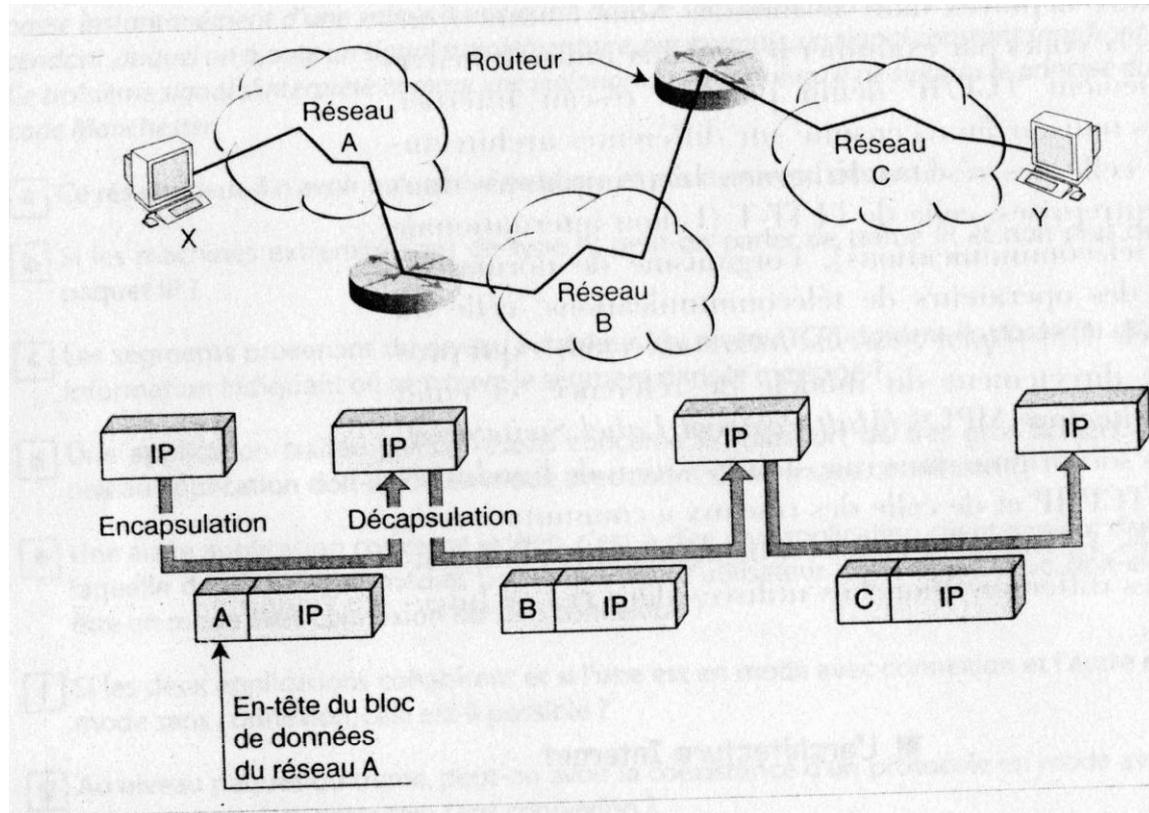
Il y a cinq architectures :

1. L'architecture Internet :

Se fonde sur l'idée de fusionner des réseaux qui veulent transporter un type de paquet unique

Adr	Données
-----	---------

Le paquet sera router dans chaque réseau jusqu'à la sortie désirée.

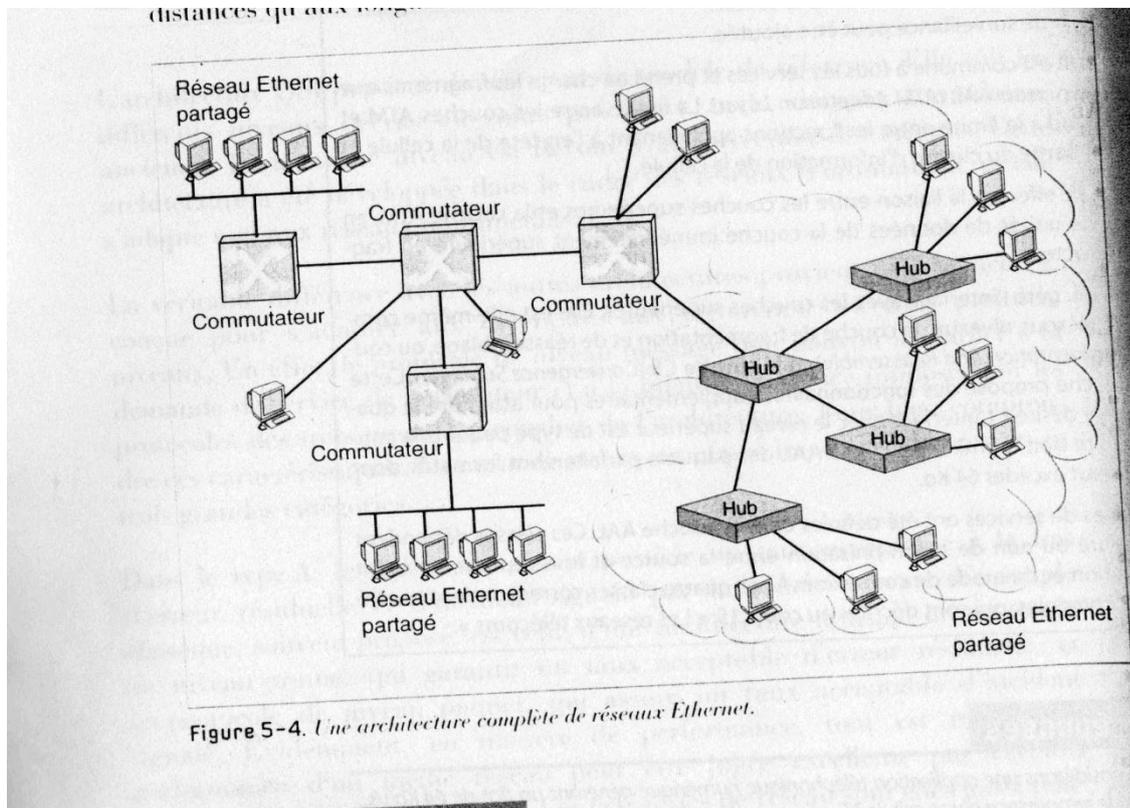


Application
TCP
IP
Accès support

La commutation de paquet.

2. L'architecture Ethernet :

A été utiliser au début pour les réseaux locaux en mode diffusion csma/cd . mais maintenant a évoluée .



Les couches supérieures				
LLC (logical link control)				
Ethernet	Jeton sur bus	MAN	Accès large bande	FDDI
La couche physique				

La commutation de circuit .

3. L'architecture UIT-T(union international de la télécommunication) :
 Utilisée par les opérateurs de télécommunication basée sur la commutation de cellule . généralement la cellule est un petit paquet de largeur fixe 53 octets.

Entête 5 octets	Données 48 octets
-----------------	-------------------

La technique de transfert appelée ATM (asynchronous transfert mode).

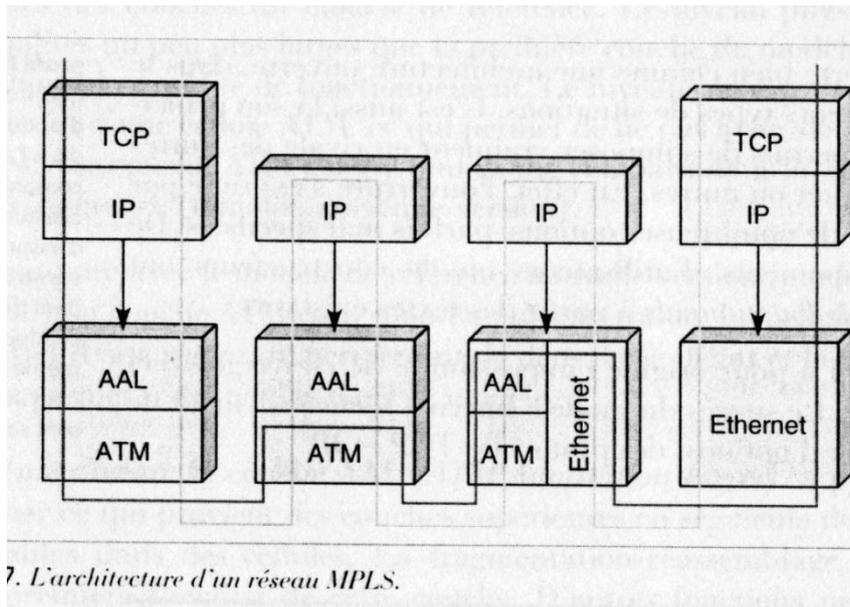
Le plan de gestion	Le plan de contrôle	Le plan utilisateur
La couche AAL(ATM adaptation layer)		
Couche ATM (asynchronous transfert mode)		
PDM physical dependent mode		

- Plan utilisateur ; transfert de donnée utilisateur .
 Plan contrôle : transfert de signalisation (ack , nack)
 Plan gestion : fonction surveillance de réseau.
 AAL : a pour rôle la fragmentation et défragmentation.
 En générale l'ATM similaire à la couche de liaison .
- Acheminement par commutation de cellule .
 - Détection d'erreur dans l'entête de cellule.
 - Multiplexage, démultiplexage .
 - Génération – extraction d'entête de cellule.

4. L'architecture MPLS :

Multi-protocol label switching :

Dans cette architecture les sous-réseaux en commutation , sont interconnecté pour des équipement LSR (label switch router) , intégrant un niveau paquet et deux niveaux frame (ATM/ethernet).



TCP	
IP	
AAL	Ethernet
ATM	
Physique	

Le routage se fait dans la couche IP/ ou au niveau ATM/ ou ethernet.

II-2-1 Eléments de théorie du signal :

La théorie du signal repose fondamentalement sur la notion de signal sinusoïdal et cela pour deux raisons essentielles :

- La réponse d'un canal à un signal sinusoïdal est facile à déterminer.
- Des signaux complexes peuvent être exprimés sous forme de fonctions simples de signaux sinusoïdaux (analyse de fourrier).

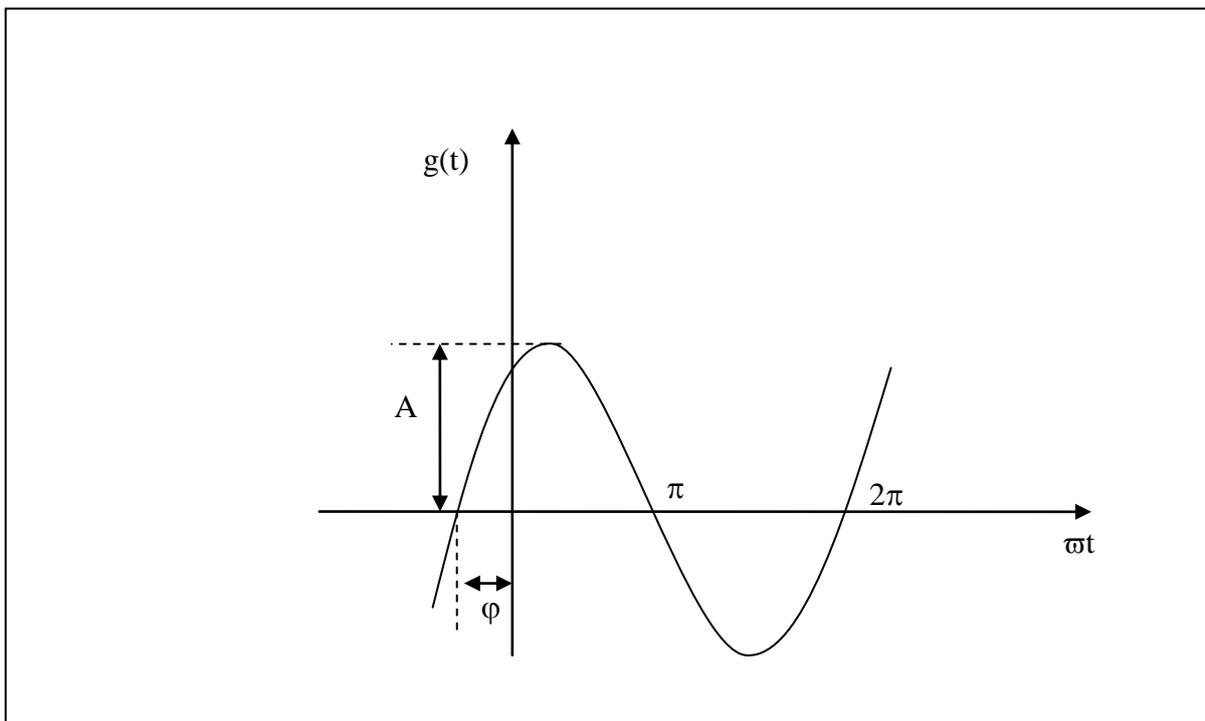
Rappelons qu'un signal sinusoïdal est un signal qu'on peut représenter par une fonction réelle de la forme $g(t)=A \sin(2\pi ft+\varphi)$

t : est une variable réelle représentant le temps.

A : est une constante représentant l'amplitude du signal

f : est un paramètre réel représentant la fréquence du signal.

φ : est un paramètre exprimant la phase ou déphasage.



En considérant ce signal $g(t)$ comme périodique (il suffit de répéter une fois sur $[T..2T]$ le signal donné sur $[0..T]$ pour obtenir un signal périodique sur $[0..2T]$) on peut le décomposer en une *série de Fourier* de la forme

$$G(t) = \frac{a_0}{2} + \sum_{n \geq 1} a_n * \cos \frac{n\pi t}{l} + b_n * \sin \frac{n\pi t}{l}$$

où

$$a_0 = \frac{1}{l} \int_{-l}^{+l} S(t)$$

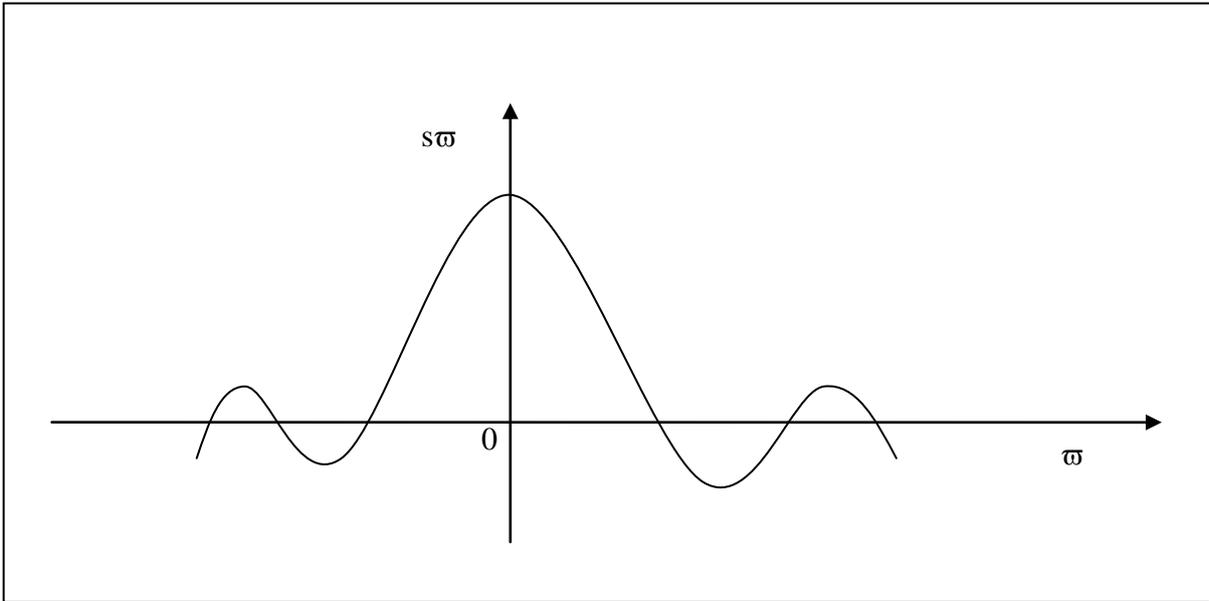
$$a_n = \frac{1}{l} \int_{-l}^{+l} S(t) * \cos \frac{n\pi t}{l} , n \geq 1$$

$$b_n = \frac{1}{l} \int_{-l}^{+l} S(t) * \sin \frac{n\pi t}{l} , n \geq 1$$

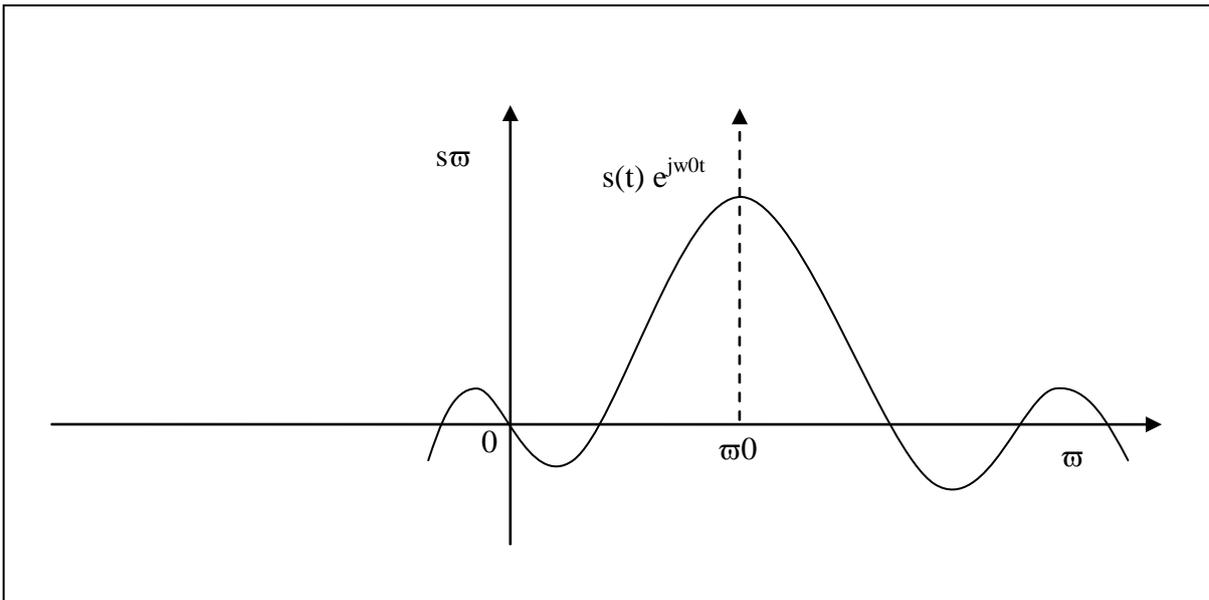
On dit que le signal carré est décomposé en une somme infinie d'*harmoniques*, la première étant dénommée *fondamentale*, et cette approximation mathématique permet de savoir quel signal électrique sera réellement reçu au bout du câble.

La transformée de Fourier possède les propriétés suivantes :

1. si c_1 et c_2 sont deux constantes et $s_1(t)$ et $s_2(t)$ deux fonctions du temps on a ensuite : $F(c_1*s_1(t)+c_2*s_2(t))=c_1F(s_1(t))+c_2F(s_2(t))$, ainsi la transformée de Fourier est une transformée linéaire.
2. si $F(s(t))=s\omega$ alors $F(s(t-t_0)) = s\omega e^{-j\omega t_0}$ le décalage dans le temps se traduit donc par un changement de phase au niveau du spectre.
3. si $F(s(t)) = s\omega$ on a ensuite $F(s(t) e^{j\omega_0 t}) = s\omega - \omega_0$ il est donc possible d'opérer un décalage en fréquence du spectre d'un signal $s(t)$ en multipliant $s(t)$ par $e^{j\omega_0 t}$



Spectre de fréquences d'un signal $s(t)$



Spectre de fréquences d'un signal $s(t) * e^{jw_0 t}$

cette figure illustre le phénomène de filtrage subi par un signal rectangulaire dont nous avons représenté uniquement la première, la troisième et la cinquième harmoniques. Il a supposé que le canal absorbe toute fréquence située au-delà de la quatrième harmonique et le signal à la sortie du canal se trouve ainsi amputé de sa cinquième harmonique.

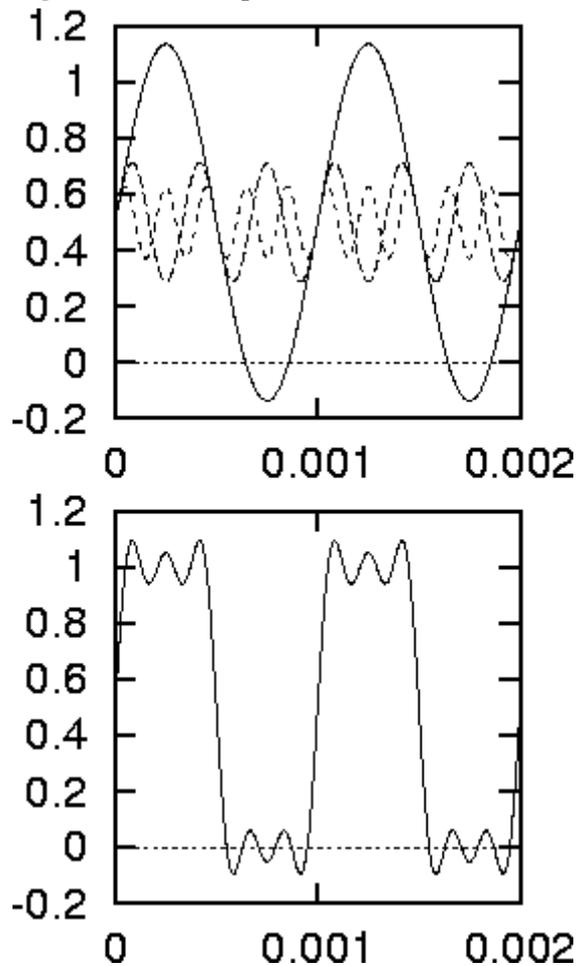
Cependant, le câble sur lequel est émis le signal possède une *bande passante* qui est l'intervalle des fréquences possibles sur ce support, donc à la réception on ne retrouve pas toute la richesse du signal initial et dans la plupart des cas le signal carré sera très déformé. Par exemple, le câble téléphonique a une bande

passante de 300 à 3400 Hz, donc tous les signaux de fréquence inférieure à 300 ou supérieure à 3400 seront éliminés.

Dans notre exemple nous obtenons

$$g(t) = \frac{1}{2} + \frac{2}{\pi} \sin(2000\pi t) + \frac{2}{3\pi} \sin(6000\pi t) + \frac{2}{5\pi} \sin(10000\pi t) + \dots$$

Figure: Harmoniques et transformée de Fourier de la séquence de bits 1010.



Dans la figure 1.7 nous trouvons à gauche les 3 premières harmoniques et on remarque que plus la fréquence augmente plus l'amplitude diminue. À droite nous avons le signal réellement reçu par le récepteur si l'on considère que le câble ne laisse passer que ces 3 harmoniques-ci. Dans ce cas le signal reçu reste assez proche du carré émis et le récepteur n'aura pas trop de mal à le décoder.

Sans entrer dans des détails relevant de la théorie du signal, nous indiquerons simplement que sur une ligne téléphonique dont la bande passante est de 3100Hz et pour un rapport signal/bruit \diamond de 10dB on peut atteindre une capacité de 10Kbits/s.

II-2 les protocoles de liaison de données .

II-2-1 : le protocoles Ethernet :

Basé sur la technique CSMA /CD Carriere sens Multiple acces / collision detection:

Chaque station ecoute le media continuellement , pour determiner quand elle aura des intervalles lui permettant d'emettre .

La collision : si deux station ou plus emettent approximativement en même moment cela entraine des collision de trame sur le support , ce qui les rendent inutilisables.

Celle-ci est reprise après un temps aléatoire, pris dans un intervalle dont la durée croît avec le nombre k de collisions non résolues

□ la durée d'émission doit être d'au moins deux fois la durée de propagation du signal

– si la trame est trop courte, il faut rajouter des bits de bourrage

– la trame minimale étant de 64 octets, la durée minimale d'émission est de 51.2 us

– pour un câblage 10Base5 (10Mbits/s coaxial)

• des segments de 500 mètres maximum

• traversée de 4 répéteurs maximum

□ en cas de collision détectée par l'émetteur

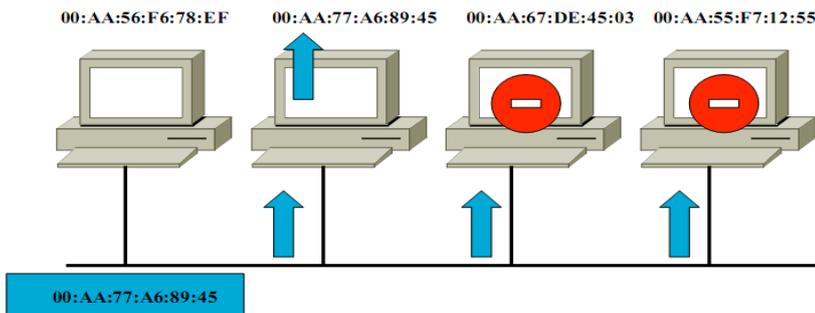
– renforce la collision par l'envoi de 4 octets (jam)

– interrompt la transmission

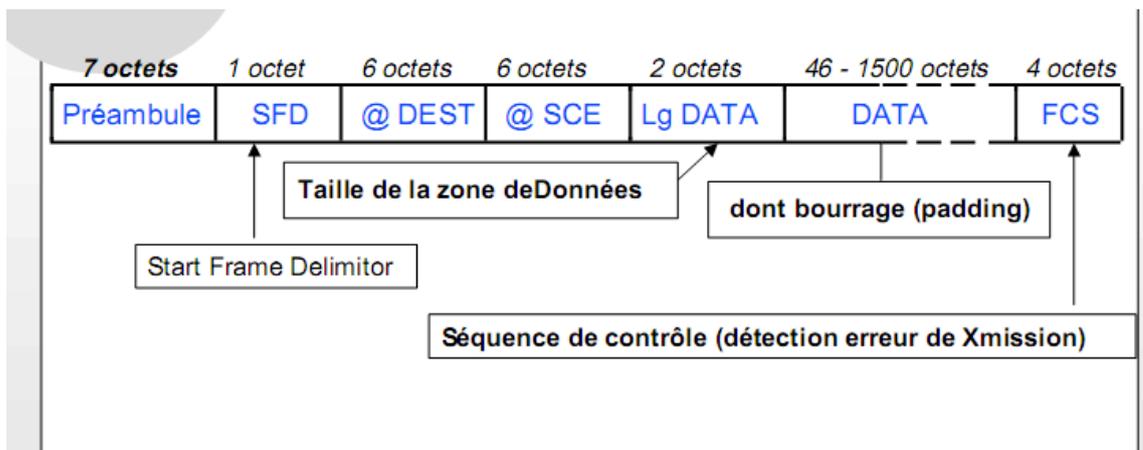
– la station attend $r * 51.2$ us ($r * \text{slot time}$) avec r entier entre 0 et $2k$, $k = \min(n, 10)$ et n est le nombre de retransmission déjà effectuées

– si $n > 15$, erreur.

La topologie physique :



Le format de trame IEEE 802.3



Champ : Préambule

• 7 octets: synchronisation

• $7 * (10101010)$

Champ : SFD (Start Frame Delimiter)

• 1 octet: 10101011

• indique le début de trame

Champ : Adresse destinataire

- premier bit (transmis)
- = 0 adresse d'une station unique
- = 1 adresse d'un groupe de stations (multicast)
- second bit (transmis)
- = 1 adresse administrée localement
- = 0 adresse administrée globalement (universelle)
- Tous les bits à 1 : adresse d'e "broadcast" ---> toutes les adresses du réseau sont concernées

Champ : Adresse source : adresse physique de la station émettrice

- premier bit (transmis) = 0 (adresse d'une station)

Format d'adresses = 6 octets (48 bits) en notation hexadécimal (0B hexa = 11 décimal) :

- 8:00:20:06:D4:E8
- 8:0:20:6:d4:e8
- 08-00-20-06-D4-E8
- 08002006D4E8

Broadcast = diffusion = FF:FF:FF:FF:FF:FF Toutes les stations d'un réseau (de tous les segments)

Les adresses MAC de IEEE sont statique , non programmable, attribué des tranches d'adresses aux constructeurs:

- Les 3 premiers octets indiquent ainsi l'origine du matériel
- 00:00:0C:XX:XX:XX : Cisco
- 08:00:20:XX:XX:XX : Sun
- 08:00:09:XX:XX:XX : HP
- 08:00:14:XX:XX:XX : Excelan

Le champ : FCS : Frame Control Sequence

- 4 octets de contrôle : CRC (Cyclic Redundancy Check)
- Polynôme de degré 32, s'applique aux champs :
 - adresses (destination et source)
 - taille de la zone de données
 - données + padding

II-2-1 : le fonctionnement

La sous couche MAC: Media Access Control

Interface entre MAC et LLC : services qu'offrent la couche MAC à la couche LLC : modélisés par des 2 fonctions :

Fonction 1 : Transmet-trame : requête LLC ----> MAC

- paramètres d'appel (@ destinataire , @ origine , taille des données , données)
- paramètre de retour status transmission = OK ou trop de collision (>16 essais).

Fonction 2 : Reçoit-trame : requête LLC ----> MAC

- paramètres de retour (@ destinataire (= propre adresse physique ou adresse, multi-destinations) , @ source , taille des données , données)

Et l'état status: soit OK ,

Soit

- Erreur de FCS
- Erreur d'alignement (pas nb entier d'octets)
- Erreur de longueur (champ taille inconsistant)

La sous couche LLC :

La sous-couche LLC a fait un appel "transmet-trame".

La couche MAC

- Ajoute préambule et SFD à la trame
- Ajoute le padding si nécessaire
- Assemble les champs: @ origine, @ destinataire, taille, données et padding
- Calcule le FCS et l'ajoute à la trame
- Transmet la trame à la couche physique :

- Si "carrier sense" faux depuis 9,6 μ s au moins, la transmission s'effectue (suite de bits).
- Sinon, elle attend que "carrier sense" devienne faux, elle attend 9,6 μ s et commence la transmission (suite de bits).

La sous-couche LLC a fait un appel "reçoit-trame".

La couche MAC est à l'écoute du signal "carrier sense", elle reçoit tous les trains de bits qui circulent sur le câble :

- Les limites des trames sont indiquées par le signal "carrier sense"
- le préambule, le SFD et l'éventuel padding .
- Analyse l'adresse du destinataire dans la trame
- Si l'adresse destination de la trame est différente de l'adresse de la station ----> ignorer
- Si l'adresse inclut la station :
- Elle découpe la suite de bits reçus en octet, puis en champs – Transmet à la sous-couche LLC les champs :
 - @ destination , @ source, taille, données
- Calcule le FCS et indique une erreur à la couche LLC si :
 - FCS incorrect
 - trame trop grande: >1526 octets (avec préambule)
 - longueur de la trame n'est pas un nombre entier d'octets (erreur d'alignement)
 - trame trop petite: < 64 octets (trame avec collision)

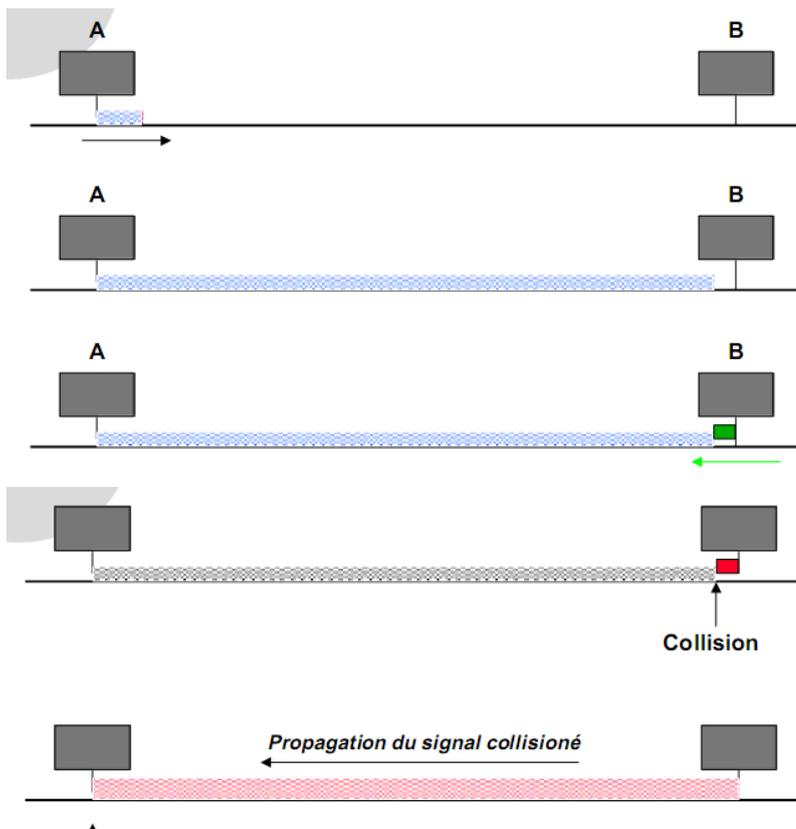
La détection de collision :

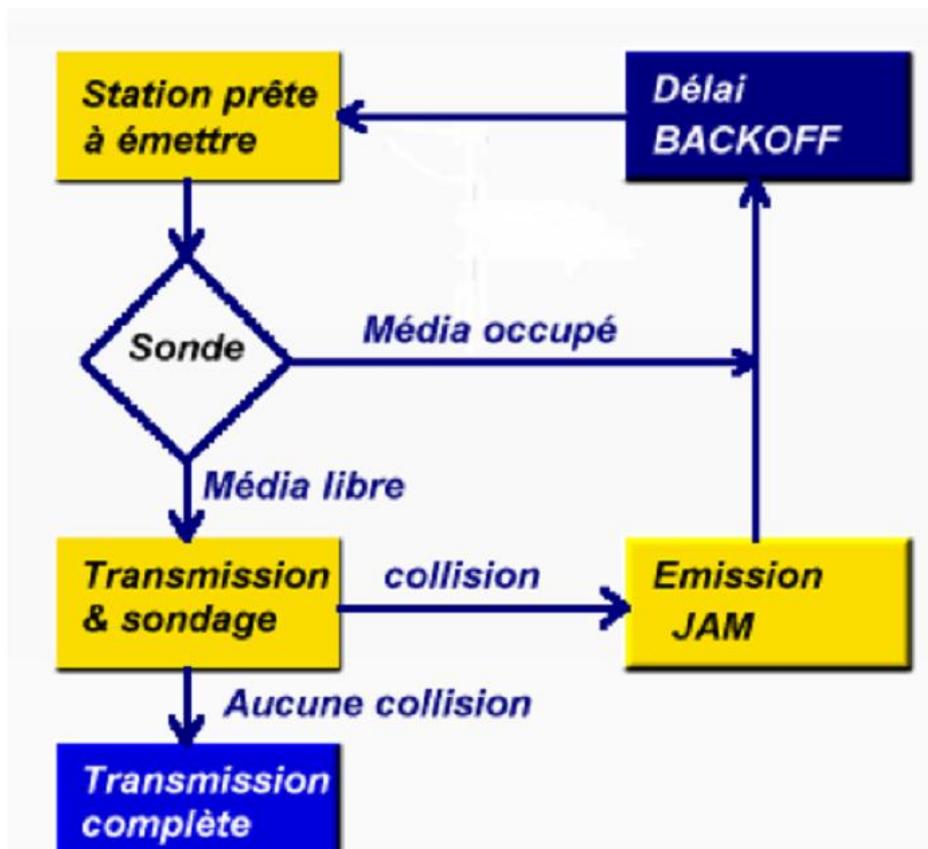
Une station regarde si le câble est libre avant d'émettre (carrier sense)

Mais le délai de propagation d'une trame sur le réseau n'est pas nul : une station peut émettre alors qu'une autre a déjà commencé à émettre

Quand ces 2 trames émises presque simultanément se "rencontrent", il y a collision

Avec un réseau très grand (et donc un temps de propagation d'une trame très long), ceci est inefficace





Minimiser le temps pendant lequel une collision peut se produire :

- le temps maximum de propagation d'une trame, temps aller et retour de la trame : le round trip delay = $50 \mu\text{s}$
- $50 \mu\text{s} \# 63 \text{ octets}$ ---> une collision ne peut se produire qu'en début d'émission d'une trame (collision window).
- On fixe un Slot time = $51.2 \mu\text{s}$ (-> 64 octets) : le temps d'acquisition du canal : une collision ne peut se produire que durant ce temps
- la station émettrice ne peut se déconnecter avant la fin du slot time (pour avoir la certitude que la transmission se soit passée sans collision)

Émetteur :

- écoute le signal "collision detection" pendant $51.2 \mu\text{s}$ (64 octets) à partir du début d'émission
- S'arrête d'émettre quand il détecte une collision en comparant le signal émis avec le signal reçu par exemple

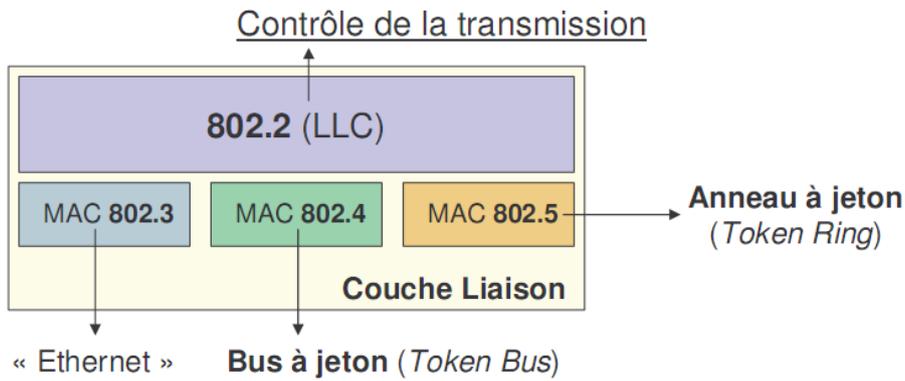
Récepteur :

- si reçoit une trame de taille inférieure à 72 octets => collision

La couche LLC transmet une trame (suite de bits) à la couche physique.

Pendant le début de la transmission (slot time = 64 octets), elle teste le signal "Collision detection" que lui fournit la couche physique

S'il y a collision, la station commence par renforcer cette collision en envoyant un flot de 4 octets (jam)



Les types de câblage utilisé

Nom		Média	Longueur max d'un segment	Nombre de nœud par segment	Longueur max d'un réseau	Avantages
10Base5	Thick Ethernet Ethernet jaune	Coaxial épais	500 m	100	2500 m	Le premier
10Base2	Thin Ethernet Cheapernet	Coaxial fin	185 m	30	925 m	Très simple
10BaseT	StarLan	Paire torsadée	100 m	1024		Utilise un hub
10BaseF		Fibre optique	2000 m	1024	1 km	Isolation galvanique entre 2 immeubles Immunité aux parasites électriques Piratage des données « impossible »
802.11		Réseau hertzien				

La méthode d'accès :

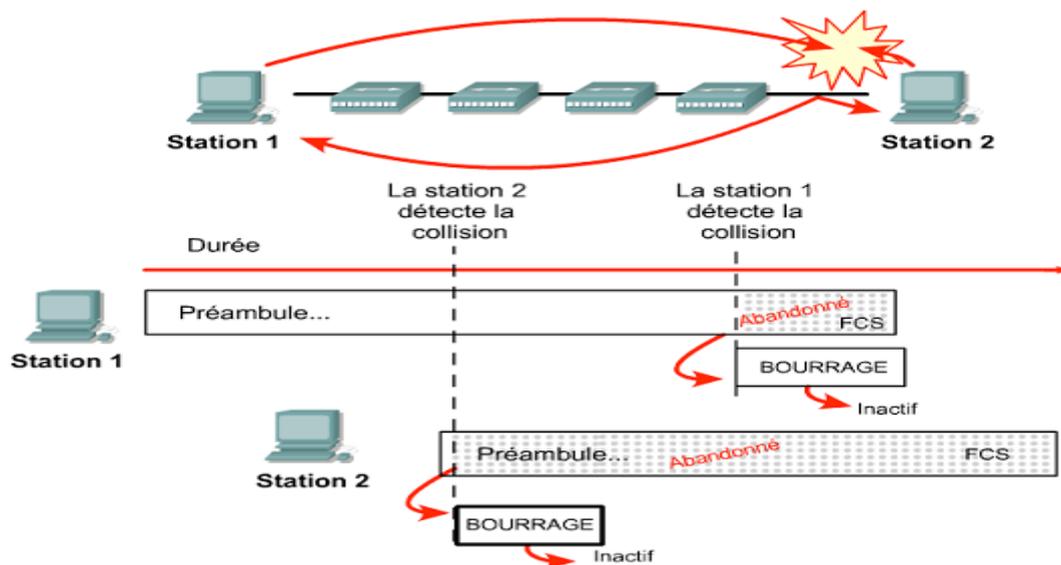
CSMA/CD: Carrier Sense Multiple Acces / Collision Detection

□ Utilisé sur toute topologie, surtout Bus (OSI 802.3 Ethernet)

□ Principe:

- Chaque station teste le signal ("porteuse") sur le support et essaie de détecter un silence de durée supérieure à t
- Après ce "silence" elle peut émettre une trame de données de taille bornée
- Si plusieurs stations émettent simultanément : Collision. Elle est détectés par analyse du signal, puis renforcée avant de suspendre l'émission
- Celle-ci est reprise après un temps aléatoire, pris dans un intervalle dont la durée croît avec le nombre k de collisions non résolues

Type de collision:



Les contraintes de CSMA/CD

la durée d'émission doit être d'au moins deux fois la durée de propagation du signal

– si la trame est trop courte, il faut rajouter des bits de bourrage

– la trame minimale étant de 64 octets, la durée minimale d'émission est de 51.2 us

– pour un câblage 10Base5 (10Mbits/s coaxial)

• des segments de 500 mètres maximum

• traversée de 4 répéteurs maximum

en cas de collision détectée par l'émetteur

– renforce la collision par l'envoi de 4 octets (jam)

– interrompt la transmission

– la station attend $r \cdot 51.2$ us (r * slot time) avec r entier entre 0 et $2k$, $k = \min(n, 10)$ et n est le nombre de retransmission déjà effectuées

– si $n > 15$, erreur.

Types d'accès :

Accès au médium équitable entre toutes les stations

Commande distribuée (sauf exception...)

– Le médium est une ressource critique partagée sur laquelle (en général) une seule station peut émettre à un instant donné.

– sous-couche MAC (Medium Access Control) de la couche 2/OSI

3 types de méthode d'accès au médium

– déterministe : AMRT, "Conteneur", Jeton

• des mécanismes de coopération ou de préallocation permettent de déterminer la station qui a le droit d'émettre

– à compétition : CSMA/CD ou CSMA/CA

• Accès multiples

• Chaque station essaie de prendre le contrôle du réseau, sans liaison avec les autres stations

– mixte : CSMA/DCR

• Début en compétition puis résolution déterministe

AMRT :

AMRT : accès multiple à répartition dans le temps

TDMA : Time Division Method Acces

Découpage du temps en périodes égales (en général) attribuées cycliquement aux stations

tranche de temps de quelques millisecondes, pas forcément utilisée

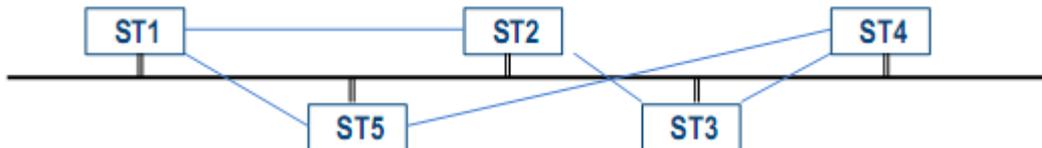
Conteneur

- Conteneur (slot, insertion de registre)
- Un conteneur de taille finie circule sur le réseau. Un bit d'en-tête indique son occupation. S'il est vide une station peut le remplir au vol. La station destinatrice le vide. Il faut gérer les trames pour garantir l'équité
- Prise active . Utilisé sur réseau DQDB (8802.6) : Cellule de 53 (48+5) octets

Jeton adressé

Jeton : méthode déterministe de base Droit d'émettre des données, durant une période bornée, est lié à la possession d'un jeton

- Quand une station a terminé une émission ou épuisé son délai, elle cède le jeton à la suivante.
- On constitue ainsi un anneau logique.



Principe: technique de réservation, le jeton est une suite d'octets (en principe 3) qui mis en circulation offre aux stations actives la possibilité d'acquiescer le droit à émettre.

Le message en circulation constitue la trame. Si le récepteur d'une trame n'a rien à émettre, il expédie explicitement une trame au communicateur de la station voisine. Ce type de technique est orientée vers les topologies en bus.

Elle nécessite dans chaque communicateur la tenue à jour de tables de routage pour décrire l'anneau logique.

Jeton priorisé:

- Utilisé sur anneau à jeton (ISO 8802.5 TokenRing IBM)
- Le jeton n'est plus adressé à une autre station mais émis avec un niveau de priorité et capté par une station de priorité supérieure ou égale
- Plus de perte de temps par station inactive ou perte de jeton par station destinataire
- Problème de perte par station qui détient le jeton subsiste
- Prise actives . Modification au vol du niveau de priorité demandée et transformation "au vol" d'une trame de jeton en trame de données
- Jeton non adressé .

Les communicateurs des stations peuvent capturer le jeton et le transformer en trame. Lorsque la trame aura terminé son périple, le communicateur de la station émettrice la retire du réseau et réémet le jeton. Cette technique est utilisée dans le cas de topologie en anneau. Il existe trois techniques de renvoi du jeton:

- renvoi du jeton après retour complet de la trame
- renvoi du jeton sur reconnaissance de l'en-tête de la trame,
- renvoi du jeton immédiatement.

Le jeton est donc sur 3 octets.

Début de Trame SD	Access control AC	ED
-------------------	-------------------	----

- **SD** (Start Definition) 1 octet.
Définition du type de la trame (jeton/données/ ou contrôle).
- **AC** (Access Control) 1 octet.
Unité de contrôle d'accès sur 8 bits donc :
 - 3 bits pour le niveau de priorité
 - 3 bits pour le niveau de réservation du jeton
 - 1 bit signification du jeton
 - 1 bit contrôle de l'octet.
- **ED** (Fin Definition) 1 octet.
Indique la fin de la trame les bits n'indiquent ici que l'Etat de la trame (défectueuse ou non).

TOKEN RING

ou IEEE802.5 ou Anneau à Jeton

1	1	1	6	6	≥ 0	4	1
Start Delimiter	Access Control	Frame control	Adresse Destination	Adresse Source	Données	FCS	End Delimiter

Le token = StartDelimiter+AccessControl+EndDelimiter

