

# CI 5 : ÉTUDE DU COMPORTEMENT DES SYSTÈMES NUMÉRIQUES

## CHAPITRE 3 – RÉSEAUX

D'après les Sciences de l'Ingénieur en PTSI – Éditions Ellipses  
Laurent Deschamps & Patrick Beynet

- Les différentes topologies et classification en fonction des distances couvertes.
- Les sens possibles de transfert, simultané ou alterné.
- L'absence ou la présence de synchronisation d'horloge entre les différents nœuds.
- Les principaux médiums avec leurs caractéristiques.
- Les différents mécanismes de gestion de conflit.
- Le modèle OSI.

Savoir

SAVOIRS :  
– **Mod - C5.1 :**

1	Caractérisation d'un réseau	2
1.1	Classification, dimension	2
1.2	Les différentes topologies	2
1.3	Quantités d'informations / Temps d'obtention	2
1.4	Robustesse d'un réseau	3
1.5	Circulation des informations	3
1.6	Mode de transmission	3
1.7	Synchronisation	4
1.8	Médium ou support physique	4
1.9	Techniques de transmission	5
1.10	Les accès au médium	5
1.11	Échanges d'informations sur le médium	6
1.12	Le modèle OSI	7
1.13	Positionnement des bus de données	7
2	Exemples de réseaux	8
2.1	Ethernet et le protocole TCP / IP	8
2.2	Le bus CAN	10
2.3	L'I2C	11
2.4	Mais encore...	13
3	Méthodes – Comment déterminer les caractéristiques d'un réseau ?	13
3.1	Détermination des éléments physiques d'un réseau	13
3.2	Détermination du type de liaison dans un réseau	15
3.3	Détermination de la structure des données	15

*Ce document évolue. Merci de signaler toutes erreurs ou coquilles.*

# 1 Caractérisation d'un réseau

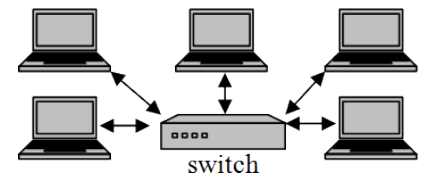
## 1.1 Classification, dimension

- **LAN** : Local Area Network. Réseau de taille locale qui permet d'interconnecter des clients du réseau d'une entreprise : de quelques mètres à un kilomètre.
- **MAN** : Metropolitan Area Network. Permet d'interconnecter plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants.
- **WAN** : Wide Area Network. Réseau de la taille d'une région à la terre. Permet à tous les LAN ou MAN de communiquer entre eux.

## 1.2 Les différentes topologies

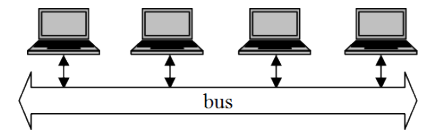
### Topologie en étoile

Un commutateur (switch) permet de connecter les équipements. Une machine perturbatrice, peut être isolée du réseau. Inconvénient : si le commutateur présente un défaut, tout le réseau est perturbé. C'est la structure actuelle d'un réseau Ethernet à paire torsadé (100 Base T, 1000 Base T).



### Topologie de type bus

Tous les équipements partagent une même liaison. Avantage : peu coûteux à mettre en œuvre. Inconvénient : la coupure du bus ou un élément perturbateur pénalise tout le réseau (10 Base 5, CAN, I2C).



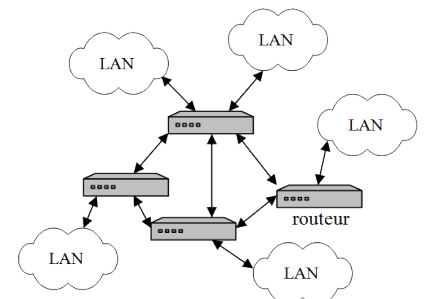
### Réseau en anneau

Chaque équipement possède un temps de parole sur le réseau. Les équipements sont connectés à un concentrateur (Token Ring) ou en bus. Une carte « maître » fixe les temps de parole. On peut représenter ce fonctionnement par un « jeton » qui passe successivement dans chaque équipement (e.g. Interbus).



### Topologie maillée

Utilisés principalement par Internet, les réseaux maillés utilisent plusieurs chemins de transfert entre les différents nœuds. Des routeurs possèdent des tables de routages. Ils déterminent en temps réel le meilleur trajet parmi tous ceux possibles. Cette méthode garantit le transfert des données en cas de panne d'un nœud ou d'une liaison saturée qui peut alors être assuré sur une autre liaison. Cette architecture est complexe à mettre en œuvre et n'est généralement pas utilisée dans les réseaux locaux.



## 1.3 Quantités d'informations / Temps d'obtention

Dans le cas de capteurs reliés à un ordinateur, des informations de un bit à quelques octets sont échangées. Le temps de latence est relativement faible, quelques millisecondes. Inversement, l'obtention de plusieurs méga octets (texte, image, vidéo) peut mettre plus de temps. La conception d'un réseau est souvent un compromis entre ces deux critères : quantité et temps. Le débit caractérise le rapport de ces deux dernières grandeurs. Il s'exprime de trois façons :

- en bits/s : nombre d'informations logiques par seconde ;
- en bauds (Bd) : nombre de symboles par seconde ;
- en hertz (Hz) : bande passante pour que la transmission des données soit fiable.

## 1.4 Robustesse d'un réseau

La robustesse vise à évaluer la capacité du réseau à continuer de fonctionner sous l'effet d'éléments perturbateurs internes ou externes. Citons quelques exemples de perturbations possibles :

- perturbations électromagnétiques engendrant des états non désirés sur les fils de connexions ;
- débit important monopolisant l'accès au médium (support physique véhiculant les données) ;
- « collisions » de données échangées ;
- nombre de nœuds connectés trop important voulant accéder au réseau.

Chacun des réseaux, à travers le médium et/ou les protocoles, apporte une solution à ces perturbations de façons à améliorer la robustesse. Une méthode couramment utilisée est le contrôle de l'intégrité d'un message par le calcul d'un CRC (Cyclic Redundancy Check : contrôle de redondance cyclique) ou d'un checksum (somme de contrôle). L'émetteur envoie sa trame incluant un champ contenant le code d'intégrité qu'il a calculé. Le récepteur en fait de même et valide ou non la trame reçue. On note aussi le contrôle par bit de parité sur la liaison RS232 par exemple.

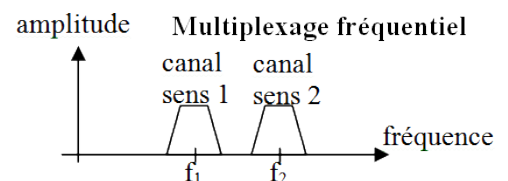
## 1.5 Circulation des informations

L'information peut circuler de différentes manières :

- dans un seul sens : liaison monodirectionnelle (émission Radio et TV, « broadcast » sur Internet) ;
- dans les deux sens mais pas en même temps : half-duplex (Talkie Walkie, CB), ;
- dans les deux sens et en même temps : full-duplex (téléphonie, Ethernet).

Le caractère half-duplex du Talkie Walkie est dû à l'utilisation d'une unique fréquence pour l'émission et la réception (et du fait que plus de deux équipements peuvent communiquer). Il est envisageable, dans le cas d'une liaison point à point reliant deux machines, d'utiliser le principe de multiplexage pour créer deux sens de transfert simultanés, et rendre ainsi la liaison full-duplex.

Le spectre ci-contre peut représenter par exemple celui de l'ADSL. Bien qu'une seule paire de fils raccorde l'abonné au central, une première porteuse permet le transport montant autour de la fréquence  $f_1$  (voire plusieurs fréquences) et le transport descendant autour de  $f_2$  (voir plusieurs).



## 1.6 Mode de transmission

### La transmission série

Une liaison série nécessite au moins deux fils (données sur un fil en half-duplex + un fil de masse), mais souvent trois : émission, réception et masse. Les bits sont transmis les uns à la suite des autres. A même médium, cette transmission sera plus robuste que la parallèle, moins chère (moins de connexions), mais n fois plus lente (n étant la largeur du mot).

### La transmission parallèle

Tous les bits du mot sont transmis simultanément sur  $n$  fils. Son coût dû aux nombres de connexions, ainsi que son manque de robustesse la limite à une utilisation pour des courtes distances. Chaque canal ayant tendance à perturber les canaux adjacents, la qualité de la transmission se dégrade rapidement avec la vitesse et la longueur de la liaison. C'est une liaison qui aujourd'hui est réservée aux très courtes distances.

## 1.7 Synchronisation

### La transmission synchrone

Dans la transmission série synchrone, les informations sont transmises de façon continue. Pour que cela soit possible, les horloges de l'émetteur et du récepteur doivent tendre à être identiques. Par contre, si les horloges sont asynchrones, bien que de même fréquence, une légère différence finit par décaler la lecture des mots.

Il est impératif de dédier un fil pour la transmission de cette horloge.

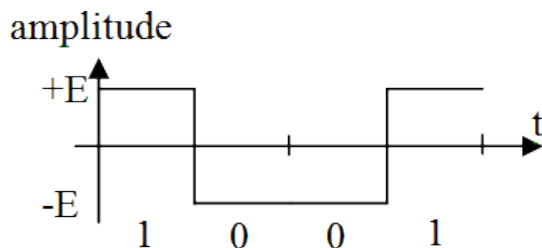
Mais le plus souvent, un codage judicieux des niveaux logiques permet de transmettre l'information d'horloge mélangée à celles des données. Le récepteur, à l'aide d'une PLL (Phase Locked Loop), extrait la fréquence du signal émis, et lit en phase les bits (ou mots) transmis. « Ethernet » est par exemple un bus synchrone. Soit grâce au code Manchester (voir en page suivante) en 10 Mbits/s, soit avec les codage MLT-3 et 4B/5B en 100 Mbits/s.

### La transmission asynchrone

Dans la transmission série asynchrone, les informations ne sont pas transmises en continu. Ceci permet d'éviter tout décalage de lecture. Les horloges de l'émetteur et du récepteur sont de même fréquence, mais ne sont pas synchronisées.

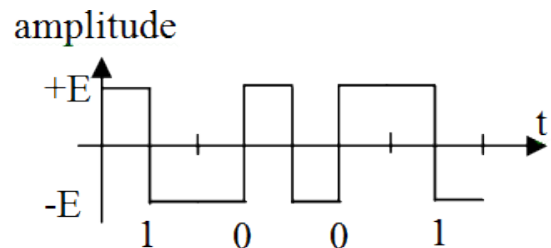
Par exemple, des bits de synchronisation « Start » et « Stop » encadrent les informations de données dans le RS232. Ils ne servent pas à ce que les récepteurs asservissent leur horloge sur celle de l'émetteur, mais à ce qu'ils identifient bien le début des bits de données ; chaque horloge sera de fréquence presque identique, avec un glissement suffisamment faible pour lire tous les mots d'une trame avant un nouveau recalage. Le codage des niveaux logiques peut permettre ou non de transporter en plus de l'information binaire, l'horloge.

Si les bits ne subissent aucun codage :



Les « 0 » sont à - 5 V et les « 1 » à 5 V. On voit que si une longue série de mêmes bits est envoyée en continu, il devient difficile de savoir combien sont émis. L'information d'horloge ne pourrait être déduite que si un « 1 » puis un « 0 » étaient émis alternativement. C'est le principe de RS232, limité à l'envoi d'un octet entre deux conditions de « Start » et de « Stop ».

Selon le codage Manchester :



Les « 0 » sont codés par des fronts montants et les « 1 » par des fronts descendants. Une longue série de mêmes bits va toujours produire des fronts, l'horloge réceptrice peut se synchroniser à l'aide de ces fronts. Il nécessite d'avoir une bande passante deux fois plus grande que le signal d'origine car il y a deux états électriques sur la ligne pour un seul état logique.

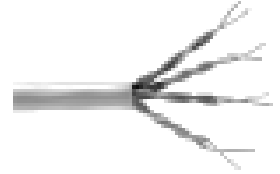
## 1.8 Médium ou support physique

Les supports physiques de transmission appelés aussi « médiums » influent sur :

- la vitesse de transmission,
- la distance possible de transmission,
- l'immunité aux perturbations électromagnétiques.

## La paire de fils torsadés

Simple à mettre en œuvre, peu coûteuse et très répandue (réseau Ethernet, réseau téléphonique), sa bande passante est de l'ordre de la centaine de mégahertz.



## Le câble coaxial

Il est composé d'un conducteur central (âme), d'un isolant diélectrique, d'une tresse de blindage et d'une protection extérieure. Il possède une bonne immunité aux perturbations, et est adapté aux transmissions à grande vitesse grâce à sa bande passante de l'ordre du gigahertz. Utilisé pendant des années pour les liaisons à très grande distance, il est maintenant concurrencé par la fibre optique.



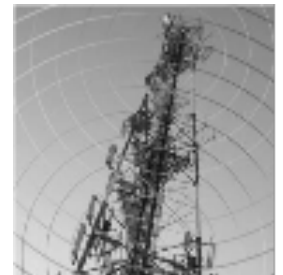
## La fibre optique

Elle ne conduit pas un signal électrique, mais un signal lumineux dans le cœur de la fibre qui peut être en verre ou en plastique. Complètement insensible aux perturbations électromagnétiques et à faible perte, la fibre optique est particulièrement adaptée aux environnements industriels agressifs, et aux transmissions longues distances. Sa bande passante est de l'ordre de 50 GHz.



## Les liaisons électromagnétiques non guidées

Elles sont la base des récepteurs/émetteurs nomades. Les ondes électromagnétiques ont l'avantage de plutôt bien se propager dans le médium gratuit et immédiatement disponible qui est l'air. Cependant, elles sont soumises à de nombreuses normes en fréquence et en puissance d'émission, et ne sont pas à l'abri de perturbations extérieures difficiles à anticiper.



### 1.9 Techniques de transmission

En fonction du médium, de ses possibilités, ainsi que du besoin de l'utilisateur, on peut utiliser trois techniques de transmission :

- la bande de base : aucune modification ou presque du signal. On envoie les bits tels quels sur le support (CAN, I2C, Ethernet, etc.),
- la transposition de fréquence : le signal de données est placé autour d'une porteuse mieux adaptée au support ou aux plus longues distances (la voix via le Talkie Walkie),
- le multiplexage temporel ou fréquentiel : cas du téléphone commuté, de l'ADSL, de la radio ou de la télévision. On profite d'une bande passante large ou d'une rapidité de transmission, pour faire passer plusieurs informations sur le médium.

### 1.10 Les accès au médium

Relier deux équipements et gérer l'absence de collision sur l'accès au médium, se fait sans trop de difficultés. Lorsque le nombre de matériels reliés augmente, il faut trouver un moyen d'arbitrer l'accès au médium.

## Le principe « Maître / Esclave »

Un élément, appelé maître, arbitre les esclaves qui peuvent accéder au support lorsque le maître les y autorisent.

Ce principe est très efficace si seul le maître a besoin de décider quand il va donner l'accès. Si un des esclaves a besoin de se manifester sur un événement extérieur, il doit attendre l'autorisation du maître. Ceci crée un temps de latence. De la même manière, le maître passe son temps à donner un temps de parole aux esclaves susceptibles d'informer d'évènements extérieurs même en leur absence (« polling »), ce qui fait perdre du temps.

L'I2C est basé sur le principe maître-esclave. Il est bien adapté aux applications audio et vidéo. En effet, dans ces dernières, le microcontrôleur (maître) passe plus de temps à diriger les esclaves, qu'à les scruter pour attendre un événement.

## Le principe de détection de collision (CSMA : Carrier Sense Multiple Access)

Il consiste à autoriser tous les équipements raccordés au bus à prendre la parole dès qu'ils en ont besoin et que le bus est libre. Tous les équipements ont le même niveau de priorité d'accès au médium. Il faut ensuite arbitrer si une collision survient après que deux équipements aient pris la parole au même moment.

Le CSMA/CD (Collision Detect) consiste à détecter la collision : le premier équipement qui détecte le conflit arrête d'émettre et envoie un signal particulier pour prévenir les autres (cas de l'Ethernet).

Dans le cas du CSMA/CA (Collision Avoidance), bien que tous les équipements aient le même niveau d'accès au médium, celui qui possède un numéro d'identification plus prioritaire conservera l'accès au bus. Ceux qui le sont moins, le détecteront et cesseront d'émettre. Le plus prioritaire continuera l'émission de son message sans avoir besoin de recommencer. C'est le cas du bus CAN.

### 1.11 Échanges d'informations sur le médium

Les échanges d'informations peuvent se faire selon trois modes.

#### La liaison point à point

La liaison point à point (P2P) est une liaison entre deux matériels uniquement.

#### Le mode client / serveur

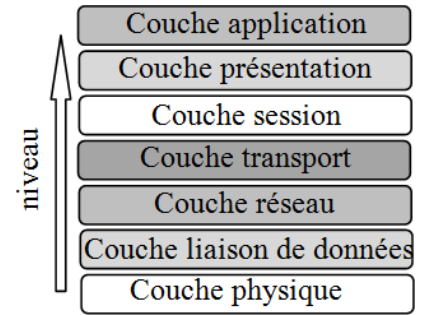
Le client demande des informations à une machine, le serveur. Ce dernier répond alors aux requêtes du client. Plusieurs matériels peuvent se connecter au serveur. Exemple : I2C ; un serveur WEB ou FTP, etc. Pour un client en mode connecté, cela peut être ramené à une liaison point à point.

#### Le mode producteur / consommateur (diffusion)

Un équipement diffuse une information, les consommateurs décident ou non d'utiliser cette information. Exemple : le bus CAN, la télévision ou la radio.

## 1.12 Le modèle OSI

Afin de rationaliser le modèle des réseaux, l'Open Systems Interconnection (OSI) a défini sept couches permettant de spécifier chaque service nécessaire au fonctionnement d'un réseau.

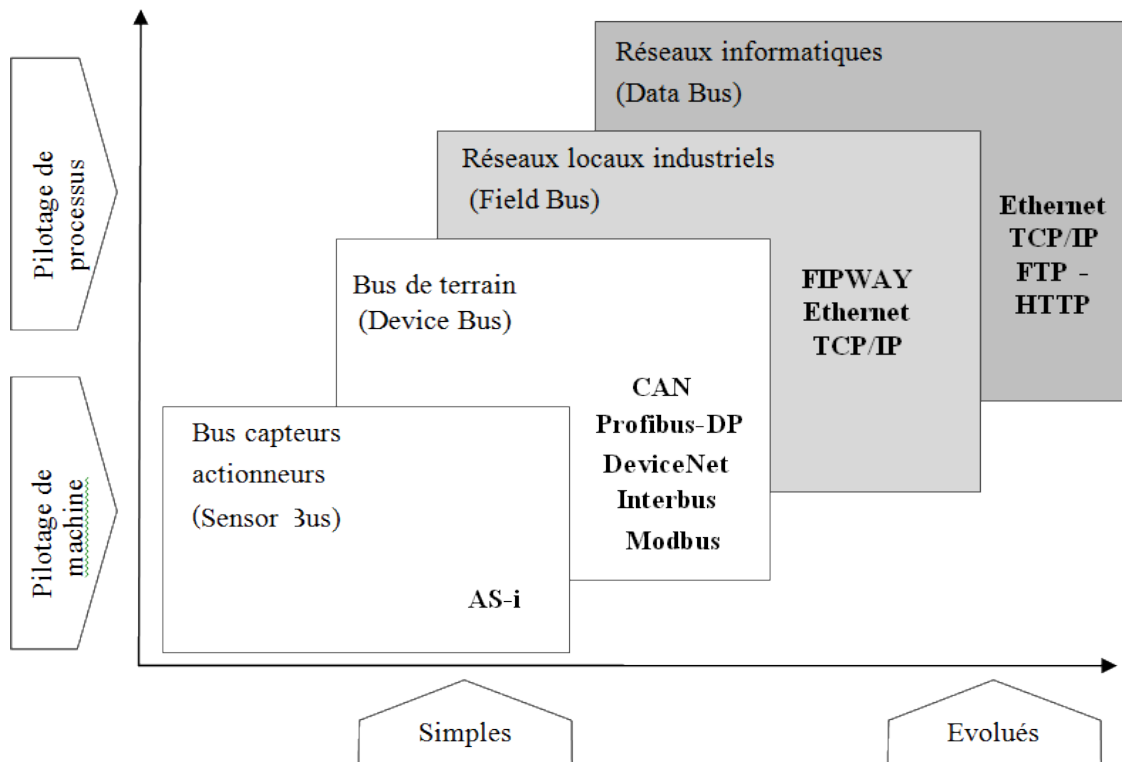


Chacune d'entre-elles a une fonction bien définie, elle se sert de services, et en propose aux couches adjacentes :

- la couche « physique » gère le codage des bits à transmettre en fonction du type de médium,
- la couche « liaison de données » fractionne les données en trame et a pour fonction de présenter des données sans erreur à la couche réseau,
- la couche « réseau » gère des paquets de données et assure le routage grâce à un adressage des matériels,
- la couche « transport » est responsable de l'acheminement de bout en bout d'un paquet de données découpé en segments de taille dépendant du type de réseau,
- la couche « session » synchronise les échanges entre tâches distantes. Elle fait le lien entre adresse logique (e.g. IP) et physique (e.g. MAC),
- la couche « présentation » traite les informations pour les rendre compatibles avec la syntaxe définie,
- la couche « application » est la partie visible pour l'utilisateur ; c'est elle qui propose les services de messagerie, internet, ftp, etc.

Le dialogue entre couches de même niveau de deux matériels connectés, nécessite l'utilisation de protocoles spécifiques.

## 1.13 Positionnement des bus de données



## 2 Exemples de réseaux

### 2.1 Ethernet et le protocole TCP / IP

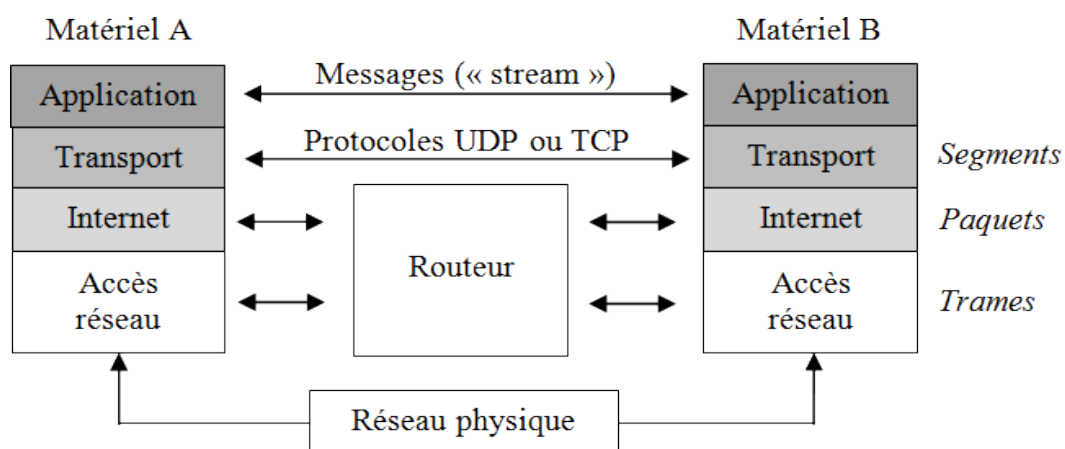
Le modèle TCP / IP (Transmission Control Protocol / Internet Protocol), créé aux États Unis, bien qu'antérieur au modèle OSI, adopte une approche modulaire. Il est possible d'établir un parallèle entre les couches des deux modèles :

Modèle TCP/IP	Modèle OSI
Couche application	Couche application
	Couche présentation
	Couche session
Couche transport (TCP)	Couche transport
Couche internet (IP)	Couche réseau
Couche accès réseau	Couche liaison de données
	Couche physique

Le TCP/IP est un protocole à commutation de paquets. L'information est découpée en plusieurs morceaux qui sont réassemblés à l'arrivée. Le chemin pour aller de la source au destinataire n'est pas établi à l'avance (contrairement au réseau dit « commuté » où la liaison physique réservée est établie à l'avance entre le destinataire et l'émetteur) et peut emprunter plusieurs chemins (réseau maillé).

Les fonctions des différentes couches sont les suivantes :

- couche « application » : englobe les applications standards du réseau (SMTP, FTP, HTTP, etc.) ;
- couche « transport » : assure l'acheminement des données ;
- couche « internet » : fournit le paquet de données (datagramme) ;
- couche « accès réseau » : spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé (Ethernet, PPP, Wi-Fi, etc.).



### Quelques protocoles « application »

- HTTP : protocole utilisé pour les serveurs web ;
- FTP : protocole pour l'échange de fichiers ;
- SMTP : protocole pour l'échange d'e-mail ;
- DNS : Permet d'obtenir une adresse IP routable correspondant à un nom de serveur.



## Les deux protocoles de « transport »

- UDP : échange de segments sans accusé de réception des données. Il est non fiable.
- TCP : plus fiable que l'UDP, il crée un mode connecté virtuel. Les en-têtes sont plus volumineux que ceux de l'UDP.

## L'adressage IP

L'IP (Internet Protocol) est un service de la couche « réseau », sans connexion et non fiable. Il est chargé d'acheminer les paquets à la bonne adresse, en utilisant le plus court chemin. On parle de routage de données.

L'adresse IP est une adresse logique « routable », donnée à chaque équipement connecté au réseau et susceptible de traiter des paquets IP. Elle permet avec son masque de définir un réseau logique, d'échanger entre deux machines (« unicast »), de diffuser à un groupe de machine (« multicast »), ou sur tout le réseau (« broadcast »). Elle est composée de quatre octets (IPv4), séparés par un point. Par exemple : 192.168.0.1.

Ce protocole possède des services qui lui sont propres :

- ARP : permet d'obtenir une adresse physique (MAC) à partir d'une adresse IP ;
- RARP : permet d'obtenir une adresse IP à partir d'une adresse MAC ;
- ICMP : permet de tester la couche IP et réseau (utilisé par la commande « ping »).

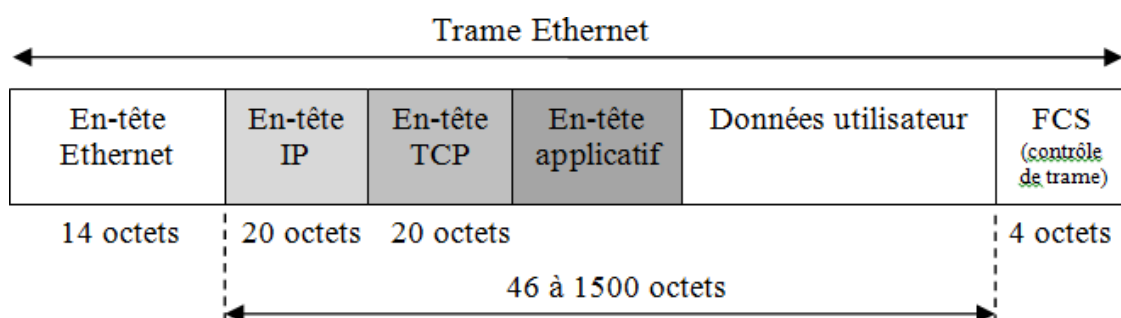
## L'adressage MAC

La couche « Accès réseau » est la couche où circulent physiquement les données sous formes de trames. Une adresse physique MAC (e.g. 08 - AB - 27 - 0C - 50 - 66) codée sur six octets, propre et unique au monde, est attribuée à chaque matériel accédant à l'Ethernet. Mais, le TCP/IP peut aussi utiliser le Wi-Fi (Wireless Fidelity) ou la paire téléphonique via le PPP (Point-to-Point Protocol) pour l'ADSL.

## L'encapsulation

Pour chaque protocole, un en-tête est ajouté. C'est le principe de l'encapsulation. L'analyse d'une trame TCP/IP Ethernet montre l'en-tête Ethernet avec les adresses MAC, puis celui IP avec ses adresses, puis le TCP ou l'UDP.

Ainsi, pour une application travaillant selon TCP/IP sur Ethernet, obtient :



## Le principe de détection de collision

Le principe du CSMA/CD (collision destructive) est utilisé sur le bus Ethernet :

- détection de la collision ;
- arrêt de la transmission de la trame ;
- émission d'une trame de brouillage ;
- attente d'un temps aléatoire ;
- réémission de la trame.

## 2.2 Le bus CAN

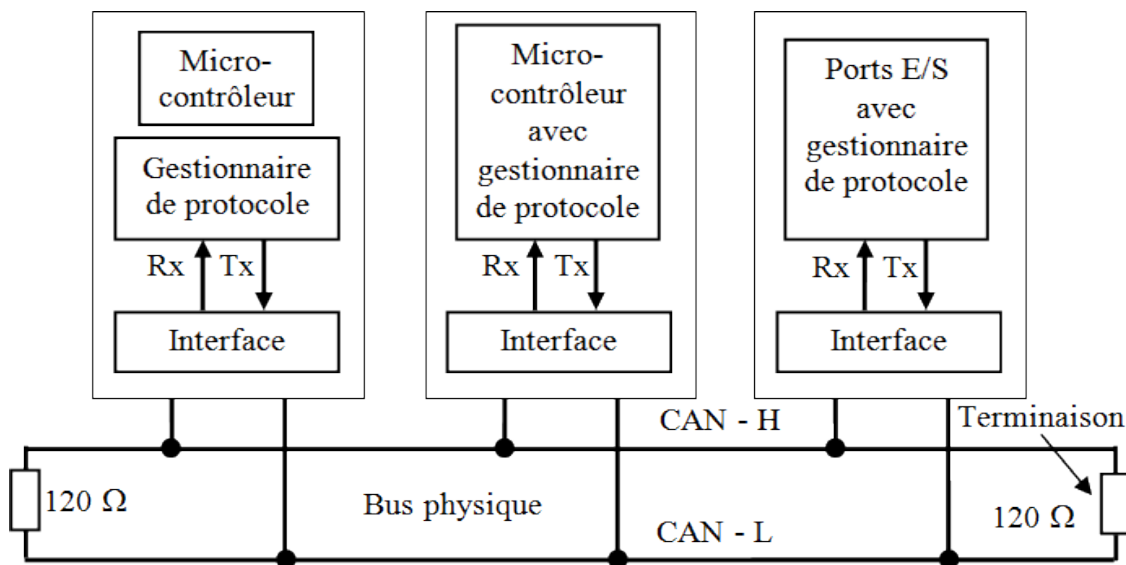
Le bus CAN (Controller Area Network) a été développé par la société Bosch pour les besoins de l'automobile. Il ne comprend qu'une partie des deux premières couches (« physique » et « liaison de données ») du modèle OSI. Sa relative robustesse aux agressions électromagnétiques lui a ouvert d'autres milieux d'applications, industrielles par exemple. Le médium le plus utilisé pour un bus CAN est une paire torsadée, mais cela n'est pas imposé par la norme.

Des terminaisons (résistance de  $120\ \Omega$ ) sont disposées à chaque extrémité de bus pour éviter les effets réfléchis.

La paire torsadée est en mode différentiel, un fil s'appelle CAN-H (High) et l'autre CAN-L (Low). Ce mode effectue une soustraction entre les deux signaux, et permet d'éliminer un parasite qui serait commun à ceux-ci.

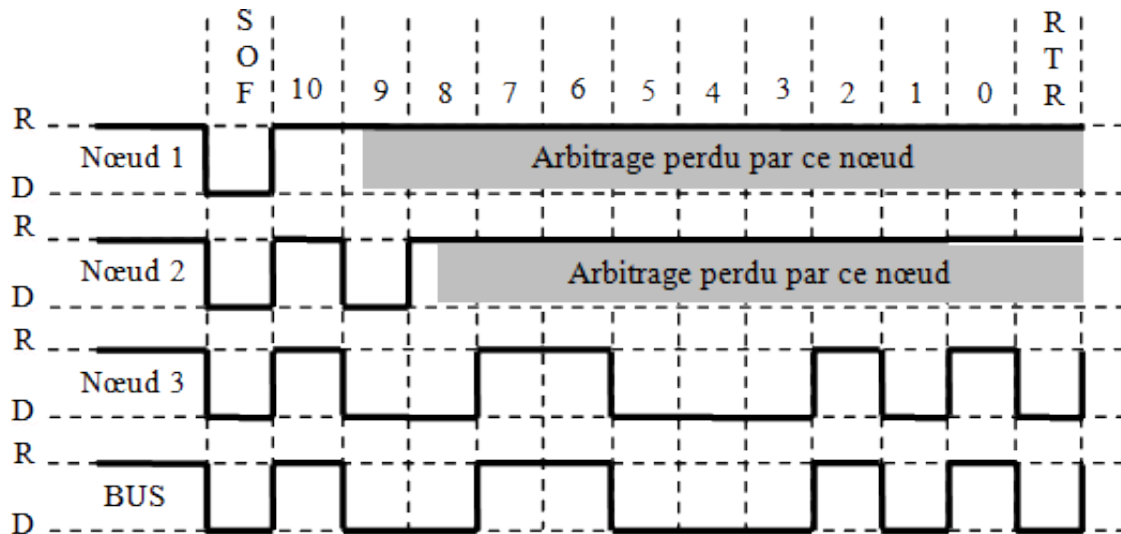
La structure de bus a été retenue avec des mécanismes permettant de prévenir les perturbations d'échange en cas de nœud défaillant.

La longueur maximale du bus est d'un kilomètre. Le débit peut aller de 10 kbits/s à 1 Mbits/s, pour une longueur de bus respectivement de 1 kilomètre à 25 mètres.



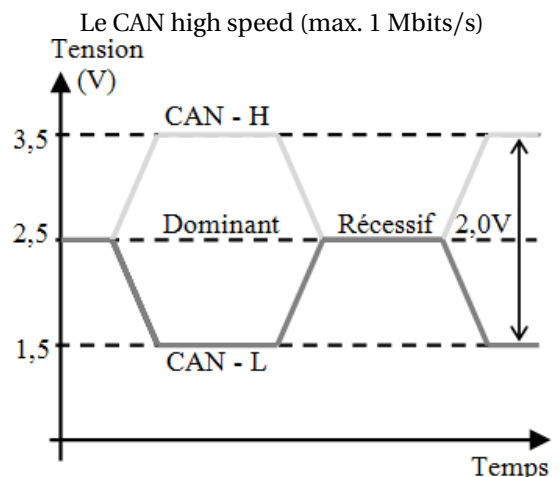
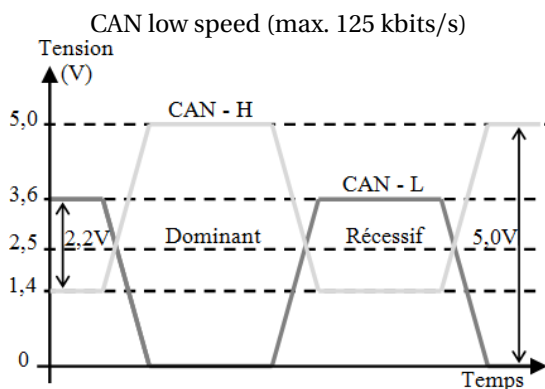
Il est possible de raccorder jusqu'à 128 nœuds sur le bus. L'accès au médium se fait sur le principe de CSMA/CA, c'est-à-dire avec détection de conflit de prise de bus sans destruction de message. Cela est rendu possible grâce au principe des bits dominants (« 0 ») et récessifs (« 1 »). Lors de l'arbitrage, le premier champ après le bit Start Of Frame (SOF), contient l'identifiant du message. Donc, le message le plus important doit avoir le numéro d'identifiant le plus faible.

Chaque nœud vérifie que le bus est libre avant d'entamer une émission. Ensuite, à chaque fois qu'il transmet un bit, il relit l'état du bus pour voir s'il est réellement transmis. S'il impose un bit dominant, il relit bien cet état. Mais s'il émet un bit récessif et qu'un autre nœud lui impose un bit dominant, il comprend qu'il n'est plus prioritaire. Il cesse alors d'émettre.



Contrairement à beaucoup de protocoles où chaque équipement possède une adresse afin qu'un message puisse être envoyé à un nœud désigné, chaque nœud émet des messages avec son identifiant mais pas l'identifiant du destinataire. Ceci est rendu possible grâce au principe « producteur / consommateur ». Dans le cas du bus CAN, cet identifiant codé sur 11 bits, est situé en début de message. Il renseigne les récepteurs sur la nature des données contenues dans chaque message. Chaque récepteur décide ensuite de consommer ou non les données.

## Chronogramme des signaux CAN-H et CAN-L



## 2.3 L'I2C

L'I2C est un bus développé par Philips au début des années 80 pour répondre au besoin croissant des échanges numériques dans l'électronique domestique, notamment dans les téléviseurs modernes : échange entre microcontrôleur, récepteur Infra Rouge, tuner, etc. Il est composé de trois fils :

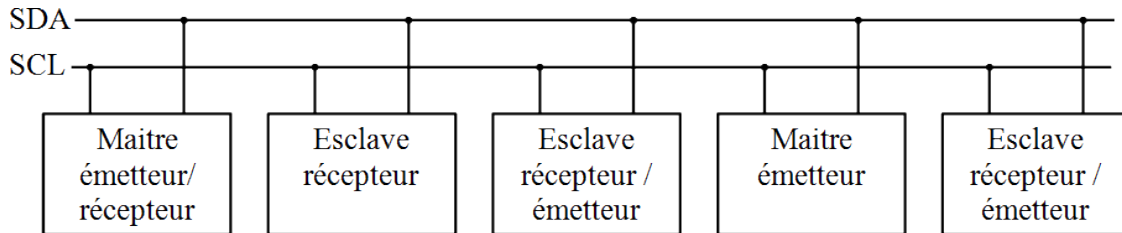
- un fil de donnée bidirectionnel SDA ;
- un fil d'horloge unidirectionnel SCL ;
- la référence de tension (Masse).

La vitesse de transmission va de 100 kbit/s à 5 Mbits/s (version 4 en 2012). Comme le bus CAN, il existe des bits dominants (niveau logique « 0 ») et des bits récessifs (niveau logique « 1 »). Cependant, cette hiérarchisation des bits n'a d'intérêt que dans le cas de multi-maîtres.

Les maîtres imposent l'horloge aux périphériques qui n'ont pas leur propre horloge interne, il s'agit donc d'une liaison synchrone. Le bus de données est unique et bidirectionnel. Les échanges ne se font que dans un seul sens à un instant donné, la liaison est donc en half-duplex.

C'est souvent un seul maître (microcontrôleur) qui interroge les périphériques. Nous sommes dans le principe du maître-esclave. Néanmoins, rien n'empêche d'avoir plusieurs maîtres, et un maître peut aussi par moment devenir esclave.

Chaque esclave doit posséder sa propre adresse. Le maître n'en a pas besoin. L'adresse est composée de huit bits. Le huitième bit précise à l'esclave si le maître veut faire une procédure de lecture (bit à « 1 ») ou une écriture (bit à « 0 »). Les adresses des composants (sept premiers bits) sont fixées en usine pour certains. Pour d'autres, susceptibles d'être utilisés en nombre sur une carte, une partie est fixée en usine, et l'autre est configurable par trois broches sur le composant.

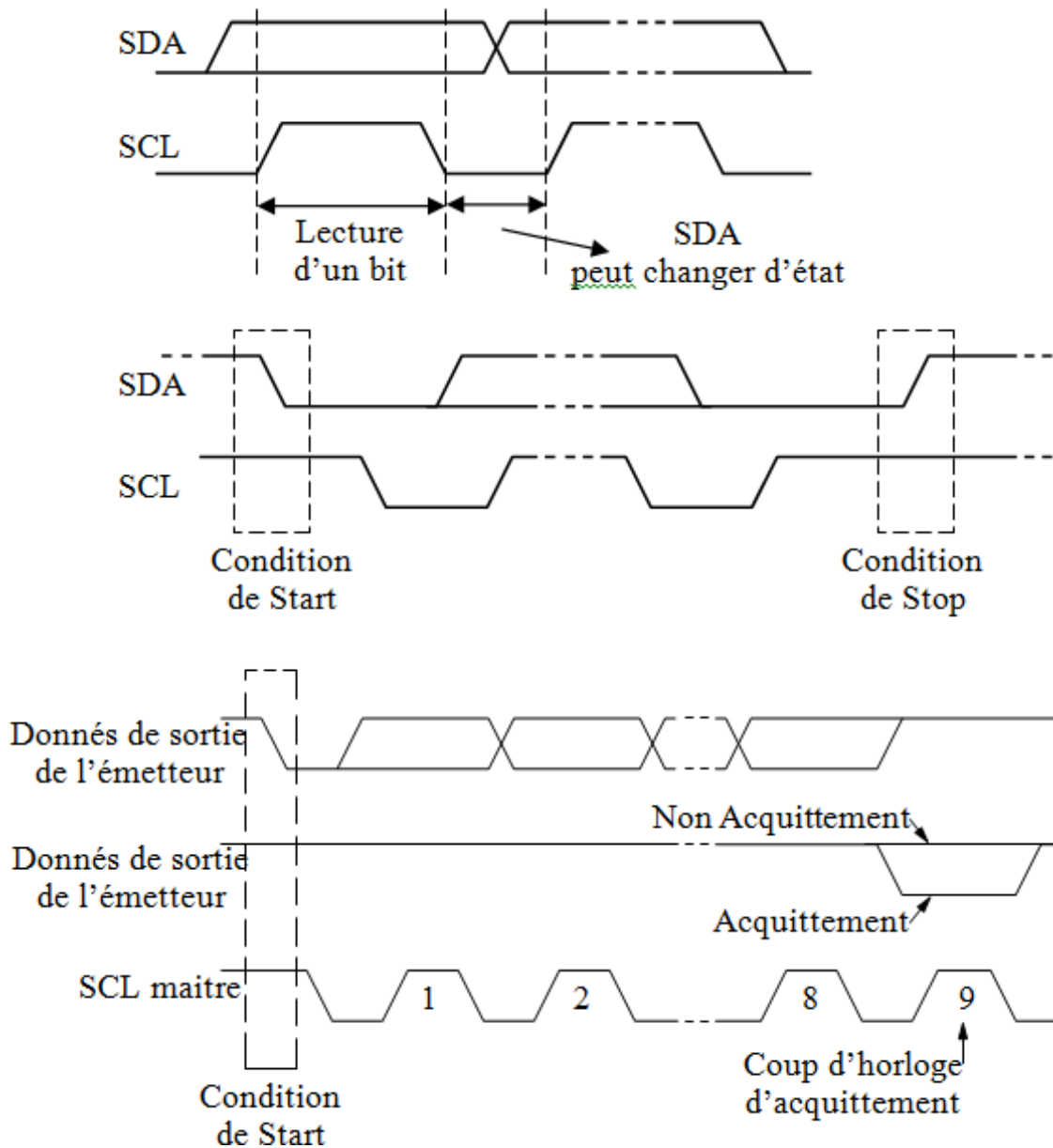


Pour utiliser le bus et interroger un esclave :

- le maître doit vérifier que le bus est libre (SDA et SCL à « 1 »),
- émettre une condition de « Start » (SDA passe à « 0 » alors que SCL est toujours à « 1 »),
- envoyer les sept bits d'adresse et ajouter le 8ème pour une lecture ou écriture,
- l'esclave précise qu'il a reconnu son adresse et émet un bit d'acquiescement.

Si par exemple il s'agit d'une demande de lecture, le maître va continuer d'envoyer un signal d'horloge, mais c'est l'esclave qui va imposer les états sur le bus de données. Pour finir un échange et libérer le bus, une condition de « Stop » doit être émise (SDA passe à « 1 » alors que SCL toujours à « 1 »).

Pour envoyer un bit, celui-ci doit être stable durant le temps où SCL est à « 1 » (variation de SDA interdit durant cette période) et peut changer d'état quand SCL est à « 0 ».



## 2.4 Mais encore...

On notera bien d'autres exemples de réseaux très utilisés : téléphonies fixe et mobile, LAN sans fil (Wi-Fi), RFID (Radio Frequency Identification pour les réseaux sans fil de capteurs), etc.

# 3 Méthodes – Comment déterminer les caractéristiques d'un réseau ?

## 3.1 Détermination des éléments physiques d'un réseau

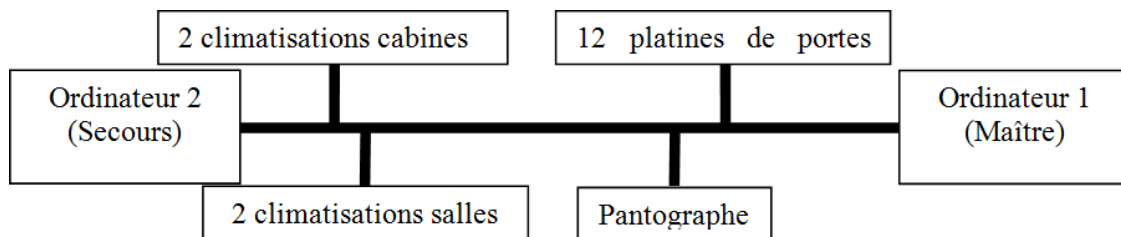
L'étude d'un réseau peut commencer par l'étude de la partie physique du réseau. Le but est de déterminer la longueur maximale de la liaison afin de déterminer si c'est un LAN, un WAN ou un MAN. La connexion entre les équipements va nous guider sur la topologie (bus, étoile). Mais celle-ci ne doit pas être confondue avec l'aspect physique. Par exemple, le 10BaseT branché sur un Hub ressemble à une topologie étoile, c'est pourtant une connexion de type Bus. Le Token Ring (topologie en anneau) lui aussi passe par un concentrateur qui ferait penser à une topologie en étoile. Pour finir, le type de médium sera à

déterminer, et aidera à connaître le type de liaison : série ou parallèle. Toutes ces informations sont à extraire des schémas et du texte présentant le réseau.

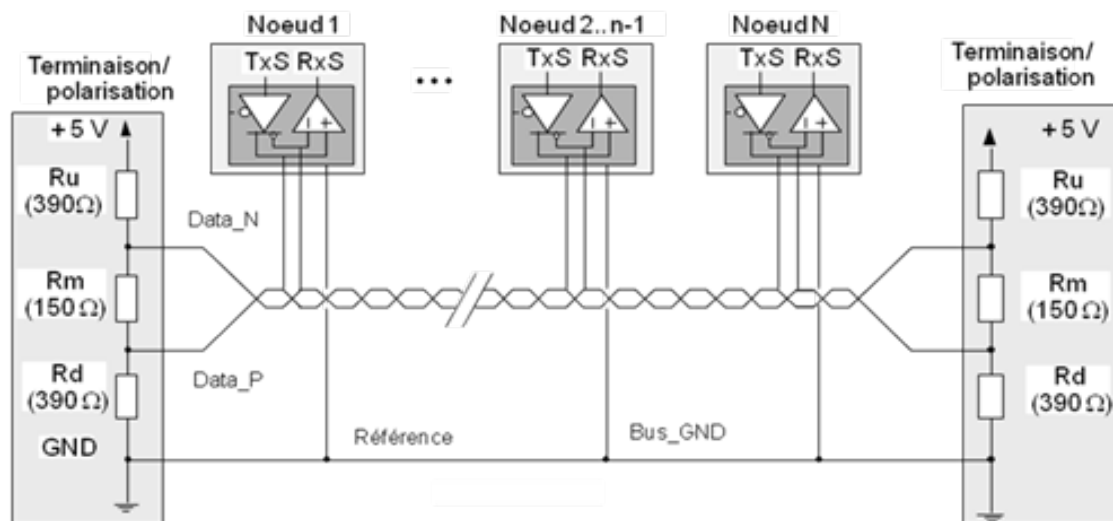
Exemple

### Bus de terrain MVB pour réseau ferroviaire

Les informations devant être transmises par l'intermédiaire du bus MVB (Multifunction Vehicle Bus) sont codifiées par les unités électroniques locales (EDCU, climatisation, pantographe, etc.) qui sont branchées sur le bus.



La norme IEC indique que ce protocole peut être utilisé sur une paire torsadée ou sur une fibre optique pour former un bus. La vitesse du bus est de 1,5 Mbits/s, avec un temps de réponse d'environ 10  $\mu$ s. Le bus peut couvrir des distances jusqu'à 2 km, découpées en portion de 200 m et de 20 m.



Ce que nous indique la lecture de la présentation de cette norme : La lecture des informations nous indique que la longueur de bus dans sa spécification ne dépasse pas les 2 km. Il fait donc partie des réseaux type LAN, plus souvent appelé bus de terrain pour ce type d'application.

Le médium supporté par la norme peut-être une paire torsadée, ou une fibre optique. Dans l'image du bus ci-dessus, on voit la représentation de la paire torsadée en mode différentiel. Ces deux supports présentent une bonne immunité aux perturbations électromagnétiques. Chaque nœud se connecte sur le médium commun à tous les nœuds et voit tout le trafic : nous avons donc une structure de bus.

Nous avons ici affaire à une paire torsadée, c'est donc une liaison série.

### 3.2 Détermination du type de liaison dans un réseau

Une fois la partie physique déterminée, il faut connaître la manière avec laquelle les équipements vont accéder aux réseaux. La liaison est-elle synchrone ou asynchrone ? Dans quel sens peuvent circuler les informations, simultanément ou non ? Comment est géré l'accès au bus et quelle stratégie est adoptée en cas de collision ?

Exemple

Bus de terrain MVB pour réseau ferroviaire

Le protocole utilisé définit la procédure d'établissement de connexion, le transfert du message, la fin de la connexion entre le maître (ordinateur) et les esclaves (unités électroniques indépendantes). Le maître interroge un des esclaves, et il attend sa réponse. Chaque élément raccordé sur le bus possède une adresse de 12 bits. Pour les platines de portes, les huit bits de poids fort sont figés et les quatre bits de poids faible sont paramétrables par la mise en place de cavaliers sur les cartes électroniques ECDU. Les bits sont transférés selon le principe du code Manchester.

En cas de réponses multiples, la collision est détectée par le maître. Une procédure d'interrogation par parité d'adresse est prévue dans la norme.

Ce que nous indique la lecture de la présentation de cette norme :

Le principe du « maître / esclave » est appliqué, arbitrant normalement l'utilisation du bus. Néanmoins, le principe de CSMA/CD est prévu dans la norme. Les bits sont émis sur le bus selon le codage de ligne Manchester, la liaison pourra être synchrone.

Pour finir, chaque nœud se connecte au bus seulement avec deux fils et émet sur le bus à l'aide d'un simple driver (porte amplificatrice de niveau logique et de son complément). Tout indique qu'aucun multiplexage n'est effectué ; à un instant donné, un seul nœud prend le contrôle du bus et tous les autres doivent écouter : il s'agit d'une liaison half-duplex.

### 3.3 Détermination de la structure des données

Une fois établie la manière dont les nœuds peuvent communiquer sur le bus, il reste à déterminer comment les données vont être organisées. Il faut que le ou les destinataires sachent que la trame est pour eux, et qu'ils puissent en extraire les données utiles.

Exemple

Bus de terrain MVB pour réseau ferroviaire

Le maître envoie sur le bus le message de 33 bits suivant :

Début trame maître	Code fonction	Adresse	Octet de contrôle
9 bits	4 bits	12 bits	8 bits

L'esclave concerné répond alors sur le bus le message de 33 bits suivant :

Début trame esclave	Données	Octet de contrôle
9 bits	16 bits	8 bits

Les messages se terminent par un signal électrique spécifique (ED : End delimiter). L'émetteur du message génère l'octet de contrôle avec un algorithme spécifique. Celui qui reçoit le message effectue la même opération et peut ainsi vérifier s'il n'y a pas eu d'erreur de transmission.

La lecture des informations logiques présentes sur les cartes ECDU se fait avec le code fonction. Exemple d'informations logiques présentes sur les cartes ECDU (codés sur 33 bits) :

Rang Bit (de 0 à 15)	Commentaire
4	Porte verrouillée = 1
10	Porte bloquée à cause d'un obstacle = 1
11	Porte entièrement ouverte = 1

Exemple d'échange : le maître désire connaître l'état de la porte 5 :

1 1101 0000	0010	0100 1000 0100	xxxx xxxx
Début trame maître	Demande d'état d'une porte	Adresse porte 5	Octet de contrôle

L'esclave répond

1 1001 1000	xxxx xxxx xxx1 xxxx	xxxx xxxx
Début trame esclave	Donnée : porte verrouillée (rang4=1)	Octet de contrôle

Ce que nous indique la lecture de la présentation de cette norme : Un en-tête en début de message permet de distinguer s'il provient du maître (requête) ou d'un esclave (réponse). On voit qu'un message émanant du maître possède l'adresse de l'esclave destinataire. Par contre, quand l'esclave répond, il n'y a aucune adresse. Elle est inutile car après la requête, le maître sait que le message émis, est la réponse de l'esclave qu'il vient d'interroger. Le maître dispose de quatre bits pour formuler une requête à un esclave. Il y a donc seize demandes différentes possibles. L'exemple donné est le quartet « 0010 » qui est la demande de l'état d'une porte. L'esclave possède seize bits pour répondre à la requête, par exemple le 4ème bit indique si la porte est verrouillée ou non. La fin de trame est constituée d'un octet de contrôle, type CRC, afin de vérifier l'intégrité du message.

## Références

[1] Laurent Deschamps, Patrick Beynet et Al., *Sciences Industrielles pour l'Ingénieur*, PTSI, Éditions Ellipses, à paraître.