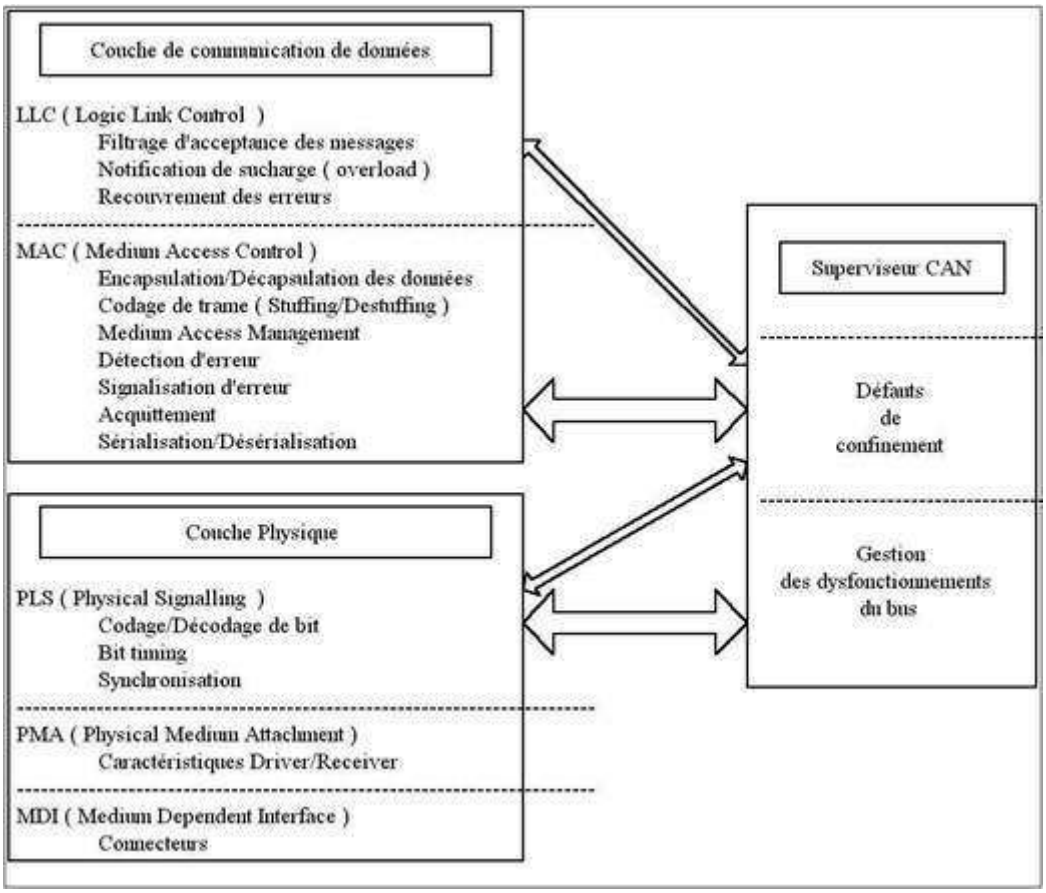
Table des matières

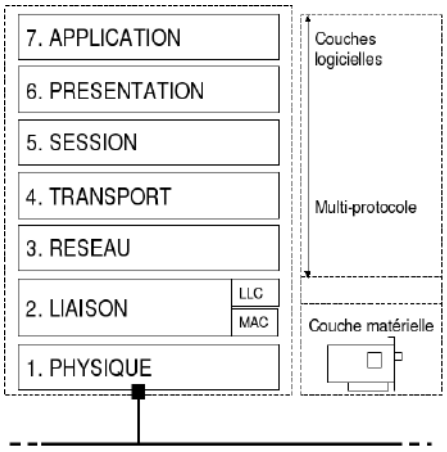


Bus CAN

Rappel

Un bus de terrain est un système de communication dédié qui respecte le modèle d'interconnexion des systèmes ouverts (OSI) de l'Organisation de Standardisation Internationale (ISO 7498 – 1983).

Le modèle OSI est une base de référence pour identifier et séparer les différentes fonctions d'un système de communication.

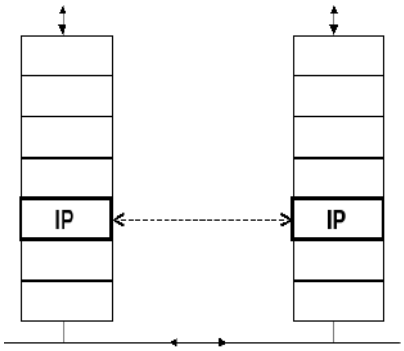


Un réseau de communication est basé sur une structure en couches.

Chaque couche (matériel, logiciel) assure un ensemble de fonctions spécifiques.

Chaque couche utilise les services de la couche immédiatement inférieure pour rendre à son tour un service à la couche immédiatement supérieure.

Un protocole est le langage commun (règles de dialogue) que doivent connaître et utiliser deux couches homologues (couche de même niveau).

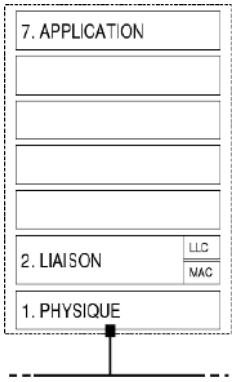


Le modèle OSI possède 7 couches ou niveaux qui définissent les fonctions des protocoles de communication qui vont de l'interface physique à l'interface des applicatifs utilisant le réseau. En raison de son apparence, la structure est très souvent appelé pile ou pile de protocoles.

Introduction

Un bus de terrain est basé sur la restriction du modèle OSI à 3 couches :

- Couche Application
- Couche Liaison
- Couche Physique



Cette modélisation est respectée par les standards de fait et internationaux.

Le standard international ISA/SP50 a en plus normalisé la partie applicative, c'est à dire la fonction d'automatisme réalisée par le système. Les concepts de la programmation objet ont été utilisés.

Les couches 3 à 6 sont vides (pas de besoin d'interconnexion avec un autre réseau, gain en performance).

La couche Liaison

Son rôle est d'assurer l'acheminement sans erreurs de blocs d'informations sur la ligne en utilisant les services de la couche Physique.

Ces fonctions principales peuvent être :

- établir et libérer les connexions ligne ;
- assurer la mise en trames et la synchronisation ;
- détecter et corriger les erreurs de transfert ;
- gérer le contrôle de flux .

La couche Liaison est découpée en deux sous couches appelées MAC (*Medium Access Control*) et LLC (*Logical Link Control*).

La sous-couche MAC

Elle gère l'accès au support, définit le format et la définition des trames et offre un ensemble de services à la sous-couche LLC.
Exemples : Ethernet 802.3 CSMA/CD, Token Ring 802.5, Token Bus 802.4, Bus CAN CSMA/CR . . . etc.

La sous-couche LLC

Elle est définie par l'IEEE 802.2 et destinée aux réseaux locaux. Elle offre à la couche réseau trois types de services :

- le service sans connexion et sans acquittement, dit de type 1 (ou mode datagramme) : la couche LLC aiguille les données vers les protocoles de couche 3. Par exemple, les réseaux Ethernet utilisent classiquement le service type 1.

- le service avec connexion, dit de type 2. Une connexion est établie entre émetteur et récepteur avant tout envoi de données. Les trames sont numérotées afin que LLC puisse garantir que toutes les trames sont arrivées à destination dans le bon ordre.

- un autre service existe, utilisé essentiellement dans les réseaux industriels : le service sans connexion avec acquittement, dit de type 3 (ou mode datagramme acquitté).

Dans tous les cas, LLC réalise un contrôle de flux. Ce contrôle permet au récepteur de commander l'envoi des trames issues de l'émetteur, afin d'éviter sa propre saturation.

LLC assure aussi un contrôle d'erreur à la réception en s'appuyant sur le champ FCS (un CRC) de la sous-couche MAC.

Remarques :
Les couches matérielles sont implémentées par la couche physique et la sous-couche MAC.
Les couches logicielles du modèle OSI vont alors de la sous-couche LLC à la couche 7 Application.

Critères du contrôle d'accès

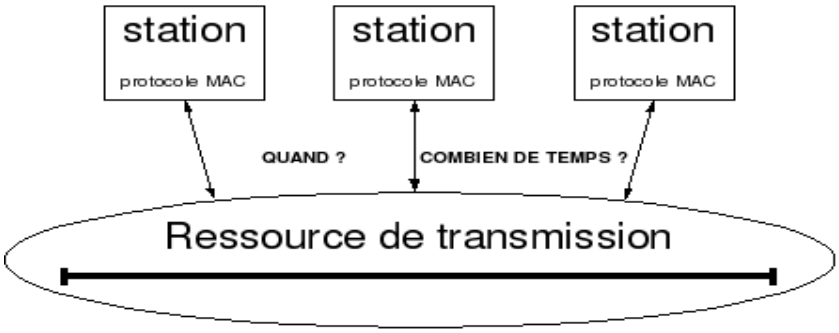
Rappel : deux stations ne peuvent disposer simultanément du média de transmission (=> collision).

- équitabilité : tous les émetteurs doivent avoir l'occasion de transmettre leurs messages
- déterminisme : tous les émetteurs doivent pouvoir disposer du média pendant un laps de temps fini, bien déterminé
- opportunité : tous les émetteurs doivent être autorisés à émettre dans un délai qui soit fonction de leur priorité
- robustesse : une erreur de communication ou la panne d'une station ne doit pas empêcher les autres stations d'accéder au média

Cas des réseaux de terrain

Les protocoles MAC sont généralement présentés en se focalisant principalement sur les "techniques d'accès à la ressource de transmission". Dans le cas des réseaux et bus de terrain, il convient aussi de présenter les principaux protocoles MAC qui peuvent être utilisés dans un **contexte temps-réel**.

- Le processus d'**arbitrage d'accès** détermine **quand** le flux de messages ou la station a le droit d'utiliser la ressource de transmission.
- Le processus de **contrôle de la durée de transmission** détermine **combien** de temps le flux de messages ou la station a le droit d'utiliser la ressource de transmission



Si on observe les systèmes existants, on constate que les protocoles MAC temps-réel mettent en oeuvre des mécanismes qui travaillent, soit sur l'accès des flux de messages, soit sur l'accès des stations (plus précisément, qui garantissent un temps d'accès borné aux stations).

En conséquence, il est possible de distinguer deux grandes classes de protocoles MAC temps-réel, selon que l'ordonnancement est mis en oeuvre sur les flux de messages ou sur les stations:

- La **classe 1** qui est relative aux protocoles réalisant un ordonnancement basé sur une assignation de **priorité aux flux de messages** (priorité traduisant les contraintes temporelles);
- La **classe 2** qui est relative aux protocoles réalisant un ordonnancement basé sur la notion d'une **garantie d'un temps d'accès borné** aux entités MAC (donc aux stations); dans ce cas, le protocole MAC offre simplement un service d'accès, en temps borné et en exclusion mutuelle, à la ressource de transmission.

Classification des méthodes d'accès

- **maître unique** : une seule station (le maître) peut démarrer un échange, les autres stations (les esclaves) ne peuvent que répondre. On distingue deux variantes : le maître gère complètement l'échange (Modbus, AS-i) ou le maître distribue un temps de parole (Fip).
  - Avantages : simple et déterministe
  - Inconvénients : panne du maître bloquante, dialogue direct entre esclaves impossible

- **pair à pair avec arbitration** : chaque station peut démarrer un échange, à tout moment, ce qui nécessite une gestion de collision (Ethernet, bus CAN)
  - Avantages : adapté au bus, extensible, efficace (pas d'attente), déterministe (bus CAN)
  - Inconvénients : non-déterministe et risque de saturation (Ethernet)

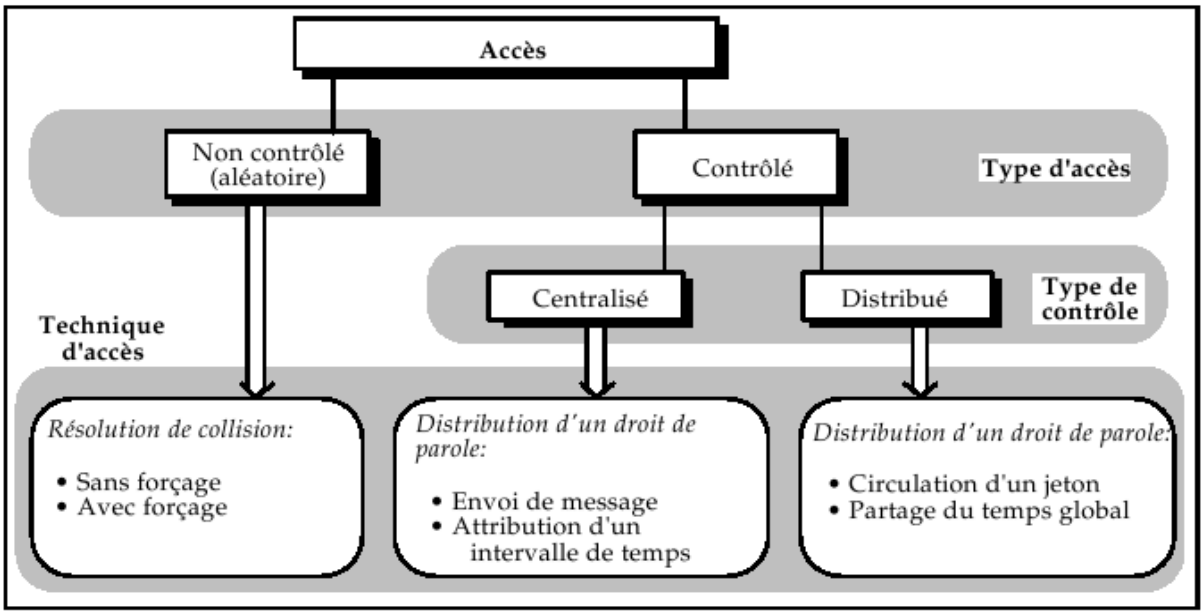
- **registre à décalage distribué (anneau)** : les stations sont reliées une à une en boucle, une seule station (maître) envoie un télégramme et chaque station y prélève ou introduit ses données (Interbus-S)
  - Avantages : déterministe et efficace pour de petites quantités de données
  - Inconvénients : panne bloquante de la liaison ou d'un station

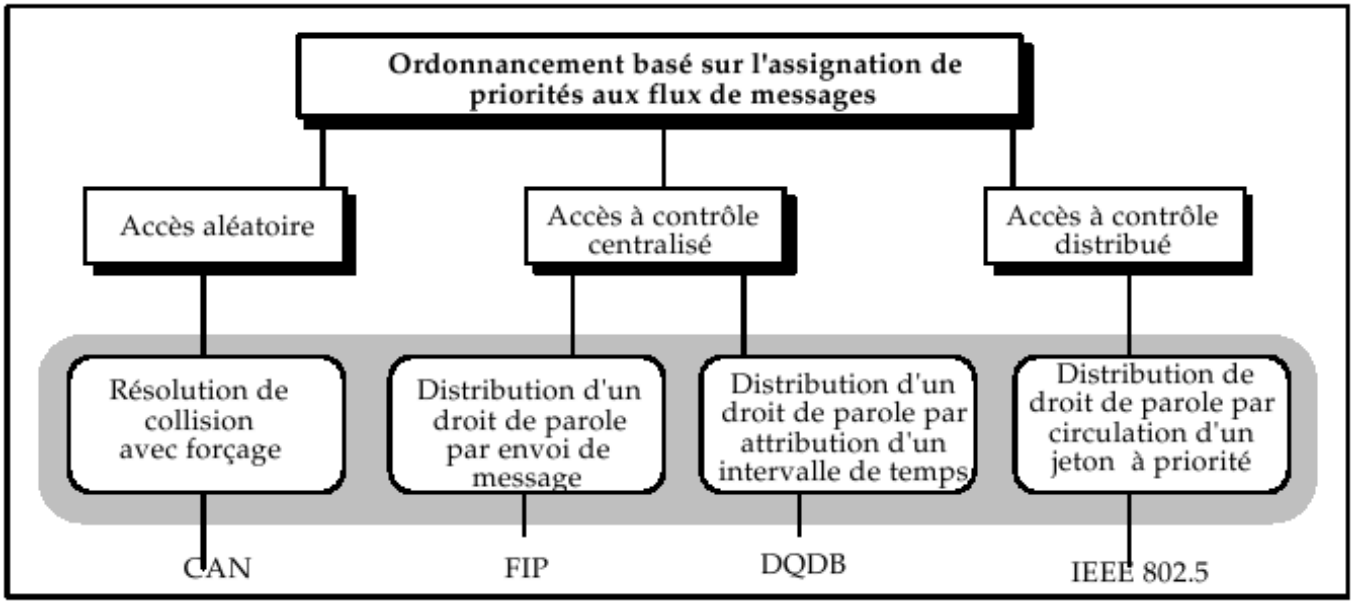
- **multi-maître (jeton)** : les stations maître se partagent un « jeton » unique, celle qui détient le jeton peut démarrer un échange et elle libère le jeton lorsqu'elle a terminé (Token Ring, Profibus)
  - Avantages : déterministe
  - Inconvénients : risque de disparition ou de duplication du jeton

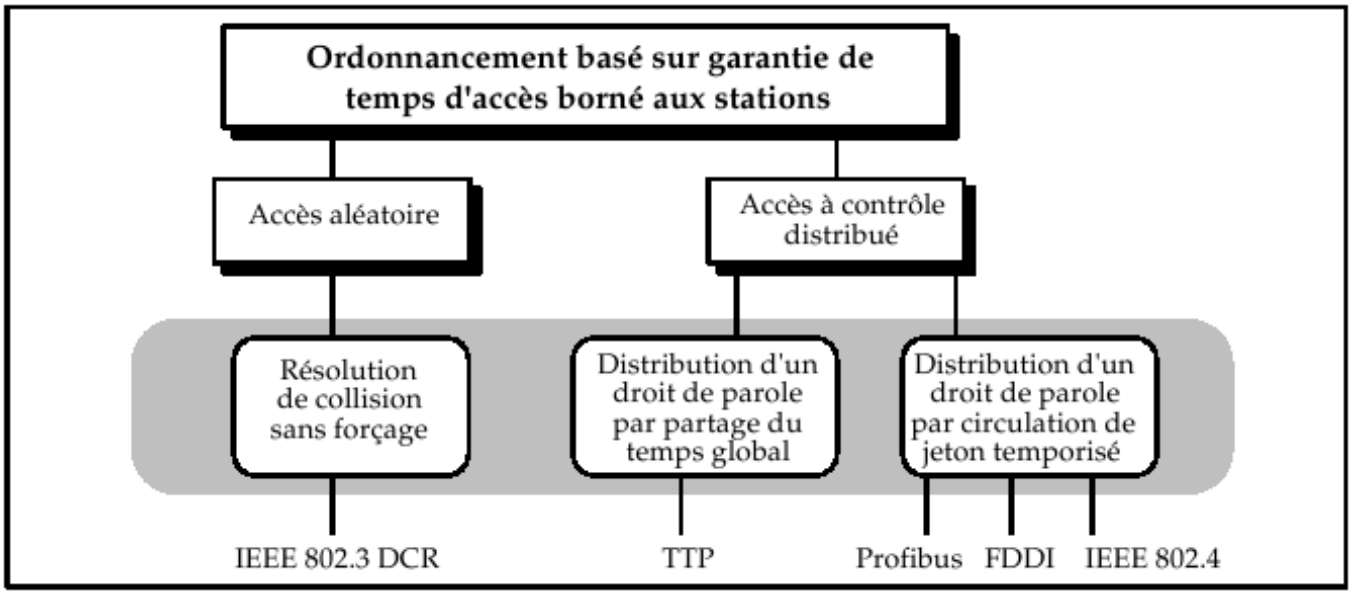
Les techniques d'accès

Les principales techniques d'accès sont :

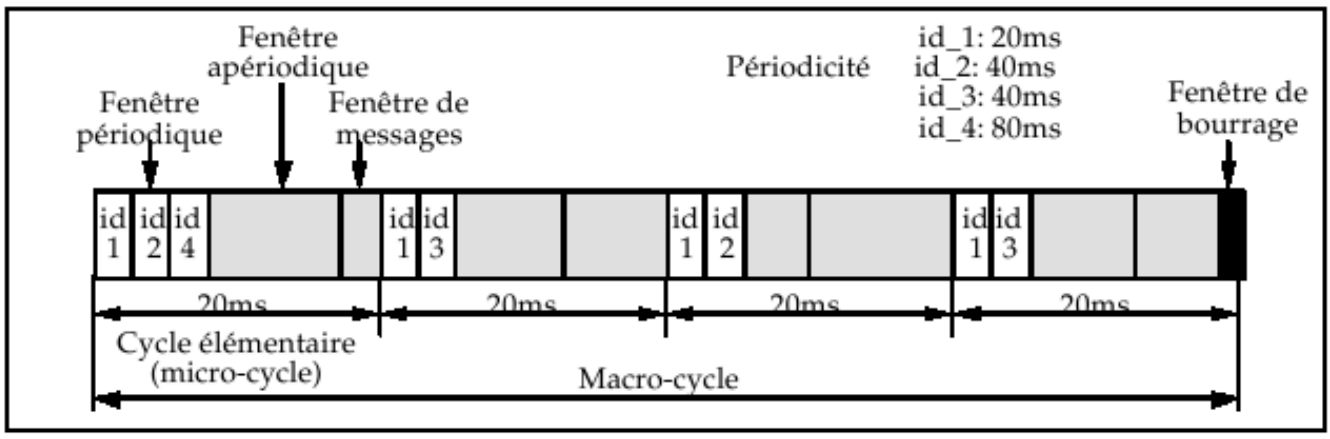
- **L'accès non-contrôlé (aléatoire)** est une technique dite de compétition qui génère, par définition, des collisions. Deux variantes, à des finalités temps-réel, de cette technique ont été définies : la **résolution de collision sans ou avec forçage.**
- **L'accès à contrôle centralisé** est basé sur l'existence d'une station de contrôle qui distribue un droit de parole aux différentes stations. On distingue deux variantes : soit la station de contrôle envoie à chaque station un message qui lui donne le droit d'utiliser le réseau ou soit la station de contrôle joue le rôle d'un horloge qui définit des intervalles de temps que les stations peuvent utiliser.
- **L'accès à contrôle distribué** est basé sur une coopération entre toutes les stations afin de définir laquelle a le droit de parole, c'est-à-dire, le droit d'utiliser le réseau. On distingue également deux variantes : la circulation d'un **jeton** (technique de jeton circulant) que les stations se transmettent; le jeton est un mécanisme de coopération explicite ou la technique de **partage du temps global**, qui est basée sur l'hypothèse que chaque station a la connaissance du temps global et des intervalles de temps où elle peut utiliser le réseau; c'est un mécanisme de coopération implicite.




Ordonnancement basé sur l'assignation de priorités aux flux de messages
Accès aléatoire
Accès à contrôle centralisé
Accès à contrôle distribué
Résolution de collision avec forçage
Distribution d'un droit de parole par envoi de message
Distribution d'un droit de parole par attribution d'un intervalle de temps
Distribution de droit de parole par circulation d'un jeton à priorité
CAN
FIP
DQDB
IEEE 802.5


Ordonnancement basé sur garantie de temps d'accès borné aux stations
Accès aléatoire
Accès à contrôle distribué
Résolution de collision sans forçage
Distribution d'un droit de parole par partage du temps global
Distribution d'un droit de parole par circulation de jeton temporisé
IEEE 802.3 DCR
TTP
Profibus
FDDI
IEEE 802.4

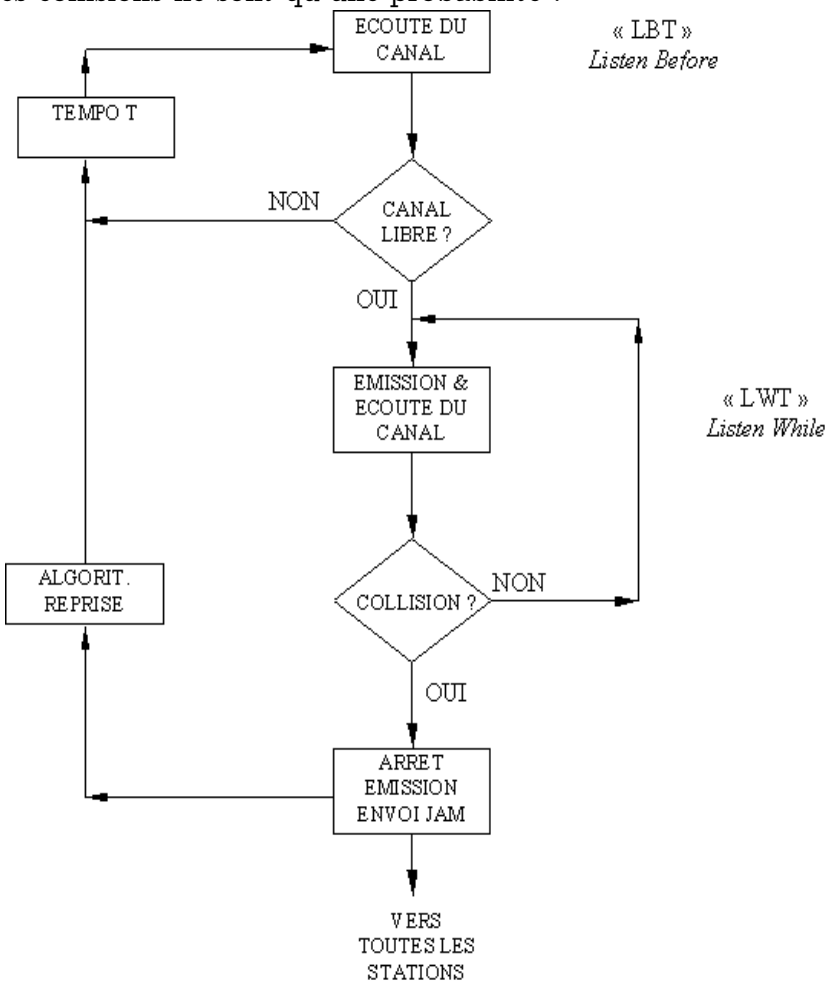
Exemple : FIP


Fenêtre apériodique
Fenêtre périodique
Fenêtre de messages
Périodicité
id_1: 20ms
id_2: 40ms
id_3: 40ms
id_4: 80ms
Fenêtre de bourrage
id 1
id 2
id 4
id 1
id 3
id 1
id 2
id 1
id 3
20ms
20ms
20ms
20ms
Cycle élémentaire (micro-cycle)
Macro-cycle

Méthode d'accès CSMA (Carrier Sense Multiple Access)

Chaque machine ayant à tout instant la possibilité de débuter une transmission de manière autonome, la méthode d'accès est dite à accès multiple (*Multiple Access* : MA). La machine observe le média en cherchant à détecter une porteuse (*Carrier Sense* : CS). Si aucune trame n'est transmise, elle ne trouvera pas de porteuse et pourra donc commencer une transmission. Elle envoie ses paquets sur le support physique et reste à l'écoute de son émission pour vérifier qu'aucune autre machine n'a suivi le même comportement qu'elle au même instant. Avec ce type de méthode d'accès, il est possible que deux ou plusieurs stations détectent le support libre (temps de propagation), décident de transmettre en même temps et ce qui provoque une collision : cette situation pose problème.

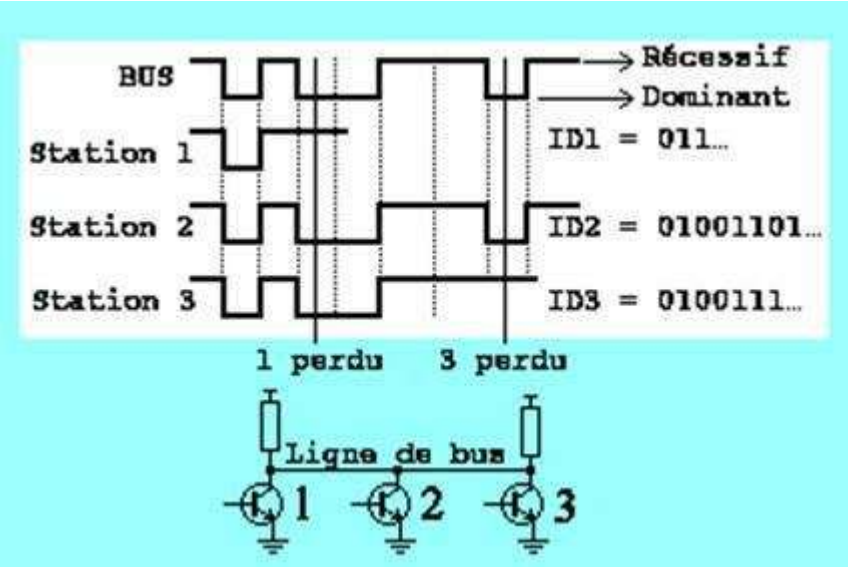
La méthode d'accès utilisée sur les réseaux Ethernet est CSMA/CD (*Carrier Sense Multiple Access / Collision Detection*). Le réseau Ethernet a décidé de s'accommoder des collisions en mettant en place un mécanisme de détection et reprise de collision (arrêt de la transmission des stations impliquées, attente d'un temps aléatoire et reprise de la procédure normale). Évidemment, on ne peut prévoir la présence et le nombre de collisions qui vont exister sur ce type de réseau. On qualifie le réseau Ethernet de **probabiliste et donc de non-déterministe**.
Remarque : on n'aura pas plus de collisions sur un réseau à 100Mbps que sur un réseau à 10Mbps puisque les collisions ne sont qu'une probabilité !



Le bus CAN utilise la méthode d'accès **CSMA/CR** (*Carrier Sense Multiple Access / Collision Resolution*). Le bus CAN relie les stations sur le principe du "ET câblé", en cas de conflit (émission simultanée), **la valeur 0 (état dominant) écrase donc la valeur 1 (état récessif)**.

On effectue alors un arbitrage bit à bit non destructif tout au long du contenu de l'émission. Ce mécanisme garantit qu'il n'y aura ni perte de temps, ni perte d'informations. Lorsqu'un bit récessif est envoyé et qu'un bit dominant est observé sur le bus, l'unité considérée perd l'arbitrage, doit se taire et ne plus envoyer aucun bit.

On qualifie le Bus CAN de **déterministe**.



Détection et correction d'erreurs

Les causes possibles d'erreurs de transmission sont dues : aux perturbations électromagnétiques et aux défauts (d'alimentation, des erreurs de conception, d'utilisation ou de montage, des conséquences de vibrations (défaut de contact), effets thermiques (trop chaud, trop froid, variations trop brutales ou trop fréquentes), des composants non conforme ou défectueux ou au vieillissement).

Remarques : même si une erreur est peu probable, elle reste possible, donc elle se produira. C'est au niveau de la couche 2 que la détection d'erreurs est la plus facile. Dans le cas des réseaux industriels, la détection d'erreurs est très importante car les conséquences peuvent être très graves (blessures voire mortelles).

Mesure d'efficacité de la détection d'erreurs

On distingue la distance de Hamming et le taux d'erreur résiduel.

La distance de Hamming entre 2 messages est le nombre de bits par lesquels ils diffèrent. La distance de Hamming d'un système de codage est le nombre minimum de bits qu'ils faut inverser dans un mot valide pour produire un autre mot valide, mais erroné.

Exemple : une distance de Hamming HD = 4

mot 1 = 0 **1** **1** 1 0 1 **0** 0 1 1 **0** 0
mot 2 = 0 **0** **0** 1 0 1 **1** 0 1 1 **1** 0

mot original	: 01100110	correct
1ère erreur	: 01100100	erreur détectée
2ème erreur	: 01101100	erreur détectée
3ème erreur	: 00101100	erreur détectée
4ème erreur	: 00101000	erreur non détectée

Il peut donc y avoir jusqu'à 3 bits falsifiés qui seront détectés à coup sûr comme erronés

Le taux d'erreur résiduel (le nombre d'erreurs simultanées détectables) : e = HD - 1

Les méthodes de détection des erreurs

On utilise une somme de contrôle (*checksum*) qui permettra de valider un message. Si le nombre d'altérations durant la transmission est suffisamment petit, alors les erreurs sont détectées. Le principe est d'ajouter aux données des éléments dépendant de ces dernières (on parle de redondance) et simples à calculer. A la réception, il est possible de réaliser la même opération sur les données et de comparer le résultat à la somme de contrôle originale, et ainsi conclure sur la corruption potentielle du message.

Remarque : l'utilisation d'une unique somme de contrôle permet la détection mais non la correction des erreurs.

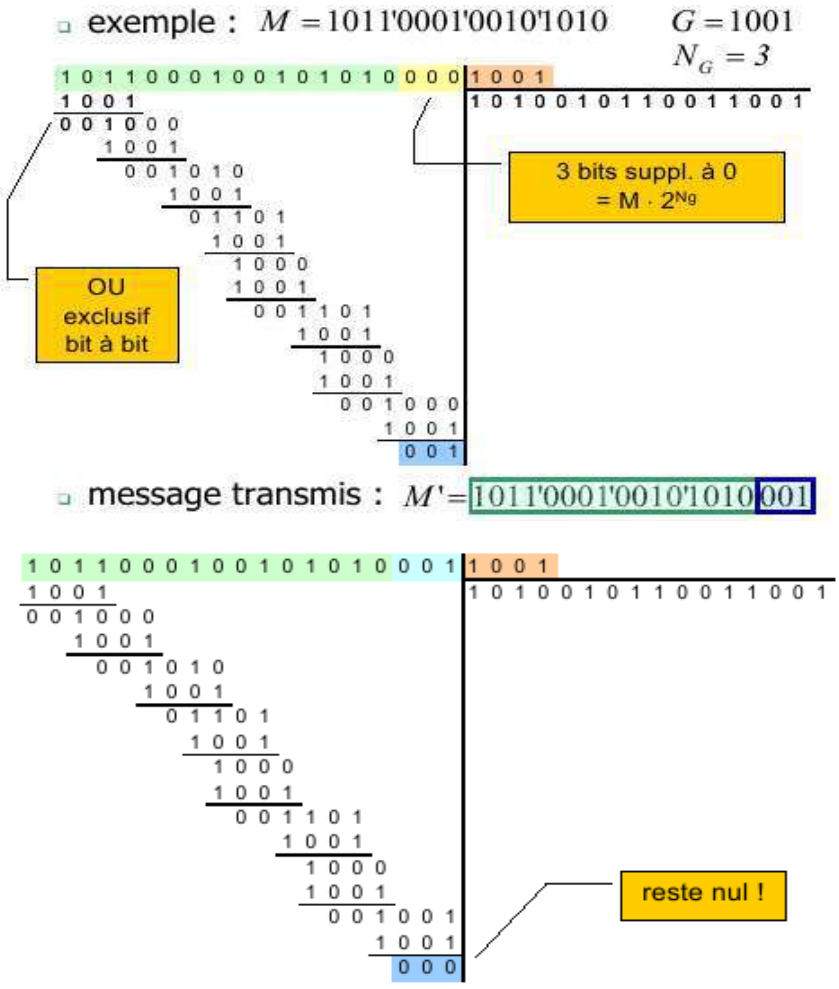
On utilise généralement soit un contrôle de parité soit un contrôle de redondance cyclique (CRC).

Le contrôle de redondance cyclique (CRC)

Un message de N bits à transmettre peut être considéré comme un polynôme de degré N-1.
Exemple : M = 1011 0001 0010 1010 soit $M(x)=1.x^{15} + 1.x^{13} + 1.x^{12} + 1.x^{8} + 1.x^{5} + 1.x^{3} + 1.x^{1}$

Le CRC est basé sur un polynôme prédéfini, le polynôme générateur G(x) de degré N_G, connu de l'émetteur et du récepteur : $(M(x) \cdot 2^{Ng}) / G(x)$

- l'émetteur effectue une pseudo-division (en fait, c'est un ou exclusif bit à bit)
- le reste est transmis à la suite du message
- le récepteur divise le message reçu par G(x) de la même manière
- si le reste de cette division est différent de 0, c'est qu'il y a eu une erreur de transmission



Les polynômes générateurs les plus courants sont :

- CRC-16 : $x^{16} + x^{15} + x^{2} + 1$
- CRC CCITT V41 (HDLC, Interbus-S) : $x^{16} + x^{12} + x^{5} + 1$
- CRC-32 (Ethernet) : $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$. Ce CRC détecte toutes les rafales d'erreurs de 32 bits et la probabilité qu'une rafale plus longue ne soit pas détectée est : $0,46 \cdot 10^{-9}$