

CHAPITRE 4

Couche liaison de données

4.1 Introduction

Les informations transportées par les supports de transmission peuvent subir des erreurs et altérations pendant l'échange des données entre deux équipements communicants. Ceci peut mener à la corruption (l'inversement de certains bits) ou la perte totale (la non-reconnaissance de la séquence) des informations échangées. Les protocoles de la couche liaison de données permettent alors de superviser et assurer la fiabilité des données transportées. Il existe deux grandes fonctions :

- La première concerne la spécification du format des unités de données échangées (trames), leur délimitation, les moyens de contrôle de leur validité, ainsi que les moyens de correction de potentielles erreurs détectées.
- La seconde permet de fixer les règles du dialogue entre deux extrémités de communication à travers l'utilisation des mécanismes de contrôle de flux et de gestion des acquittements. HDLC ((High level Data Link Control)) et PPP (Point to Point Protocol) sont deux exemples de protocoles de cette couche [8].

4.2 Format des données échangées

Les protocoles de liaison de données travaille sur des blocs d'éléments binaires appelés **trames**. Une trame est composée d'un ensemble de champs portant des suites binaires dont chacune a sa propre interprétation indiquée dans la définition du protocole. Un point très important permettant de structurer la communication entre des machines distantes est les délimitations de début et de fin de trame. Les deux solutions de délimitations les plus répondues sont : **la délimitation par une séquence binaire spéciale ou l'indication explicite de la longueur de la trame**.

4.2.1 Délimitation par une séquence binaire spéciale

Cette technique est basé sur l'utilisation d'une séquence binaires spécifique appelée Fanion (ou en anglais flag), permettant de délimité le début et la fin de la trame. Cette séquence est de taille d'un octet ayant la forme : **01111110**.

Pour éviter de retrouver cette séquence de fanion à l'intérieur d'une trame pendant l'échange de données, les extrémités de communication doivent appliquer **un mécanisme de transparence**.

- À l'émission, l'émetteur doit insérer un bit de 0 après chaque rencontre de cinq bits consécutifs de valeur 1.
- En réception c'est l'inverse, le récepteur doit supprimer le bit 0 si ce dernier est rencontré après chaque cinq bits consécutifs de valeur 1.

Avec tel mécanisme on ne retrouve jamais plus de cinq bits de valeur 1 dans les champs de la trame appart les deux fanions.

4.2.2 Délimitation par transmission de la longueur du champ de données

Cette méthode est basée sur la réservation d'un champ particulier dont sa valeur permet d'indiquer le nombre d'octets utiles contenus dans la trame.

Contrairement à la première méthode où la longueur des trames est illimitée, cette technique délimite la taille des trames selon la valeur indiquée dans le champ réservé à cette fin. Exp, si la longueur de ce champ est deux octets, la taille limite des données utiles contenues dans la trame est égale à 65536.

4.3 Méthodes de détection des erreurs

Les méthodes de détection des erreurs sont basées généralement sur l'ajout d'une suite d'éléments binaires supplémentaire (appelée aussi redondante) au niveau du code ou dans un champ spécifique à la fin de la trame. Cette suite insérée à l'émission permettra au récepteur de contrôler l'information contre les erreurs.

4.3.1 Contrôle au niveau du code

4.3.1.1 Détection basée sur la parité transversale

Cette technique de détection consiste à rajouter une information redondante au niveau du code. Elle est applicable lorsque l'échange des données se fait par caractère. A chaque caractère on ajoute un bit de contrôle (dit aussi de parité verticale ou VRC (Vertical Redundancy Check)).

Le principe de fonctionnement de cette technique est simple : à l'émission et pour chaque caractère (de 7 bits) on calcule la somme modulo 2 de ses bits. Si le résultat obtenu est paire, la valeur 0 est insérée à la fin du caractère, par contre s'il est impaire, on ajoute 1. Quant à la réception, le récepteur recalcule de son côté la parité sur les 7 bits du caractère et la compare avec la valeur du 8^{eme}. Il n'y aura pas d'erreurs si les bits de parité calculée et émise sont identiques.

Remarque : Le point faible de cette méthode de détection est qu'elle est incapable de détecter les erreurs doubles.

4.3.2 Contrôle au niveau de la trame

4.3.2.1 Détection basée sur la parité transversale et longitudinale

Pour renforcer le contrôle de validité des données échangées en utilisant le contrôle par parité, nous pouvons associer la technique de contrôle de parité longitudinale ou LRC ((Longitudinal Redundancy Check) avec la méthode transversale (VRC + LRC).

Cette technique fonctionne comme suit : à l'émission on calcule la parité transversale de chaque caractère, puis la parité horizontale de tous les bits de même rang. La transmission des caractères s'effectue en commençant par les poids faibles de chaque caractère suivi par sa parité transversale, et le dernier est suivi du code LRC obtenu. À la réception, le récepteur compare la parité émise avec le message avec une nouvelle recalculée de son côté. L'information est considérée comme valide si les deux valeurs sont identiques.

Remarque : Cette méthode ne permet pas de détecter les erreurs groupées.

4.3.2.2 Contrôle polynomial (code à redondance cycliques (CRC))

Contrairement aux méthodes précédentes, le contrôle polynomial est l'une des méthodes de détection basées sur la parité qui permet de détecter les erreurs groupées.

Le processus de fonctionnement de cette technique est résumé dans les étapes suivantes :

1. D'abord la suite binaire à transmettre (la trame) se transforme en polynôme noté $P(x)$ obtenu à travers la multiplication des valeurs des bits de la suite par une variable X levée à la puissance de leurs rangs correspondants (le rang du poids faible est égal à zéro). Par exemple, le polynôme résultant de la suite 10110101 est : $P(x) = x^7 + x^5 + x^4 + x^2 + 1$.
2. On choisit un polynôme générateur noté $G(x)$ de degré r (CRC-CCITT, CRC-12,CRC-16).
3. À l'émission, on multiplie $P(x)$ par x^r et on effectue la division euclidienne du polynôme obtenu par $G(x)$. On s'arrête quand le reste de la division noté $R(x)$ est de degré strictement inférieur à r . Ce dernier est rajouté à la fin de la trame comme information redondante. Alors, la séquence finale à transmettre, noté $M(x)$, est : $M(x) = P(x) * x^r + R(x)$.
4. À la réception, le récepteur divise le polynôme $M(x)$ reçu par le même polynôme générateur $G(x)$ utilisé à l'émission. Si le reste de la division est nul, le circuit n'a introduit aucune erreur sur l'information échangée et, par conséquent, on la considère comme correcte.

4.3.3 Correction par retransmission

On a vu dans les sections précédentes qu'au cours de la transmission sur un canal physique le taux de perte de bit (Bit Error Rate (BER)) est toujours supérieur à zéro. Il existe plusieurs façons de perte de paquets dans un réseau dont quelques-unes sont énumérées ci-après :

- La couche MAC peut détecter une erreur dans une trame (voir section 4.3).
- Débordements des buffers (des paquets peuvent s'écraser dans des bridges, des routeurs du réseau).
- Expiration du Time To Live (TTL)(des paquets qui bouclent à l'infini et sont tués).

Dans la section suivante nous présentons quelques protocoles permettant de gérer la retransmission de l'information erronée.

4.3.3.1 Transmission avec arrêt et attente (Stop & Wait)

l'émetteur est interdit d'envoyer une nouvelle trame jusqu'à qu'il s'assure que la précédente est correctement reçue par le récepteur. Une copie de chaque trame émise est gardée dans des buffers chez l'émetteur et ce dernier ne la supprime pas jusqu'à la réception de l'acquiescement correspondant.

Le récepteur doit impérativement acquiescer la bonne ou la mauvaise réception de la trame. Si le temps de réponse dépasse le délai de garde armé par l'émetteur, ce dernier procède à la réémission de la trame (voir figure 4.1(a)).

4.3.3.2 Transmission continue

Contrairement à la méthode précédente, la transmission continue permet à l'émetteur d'envoyer plusieurs trames consécutives en attendant un acquiescement. En effet, l'émetteur garde une copie de tous les trames émises jusqu'à la réception de leurs acquiescements correspondants (voir figure 4.1(b)).

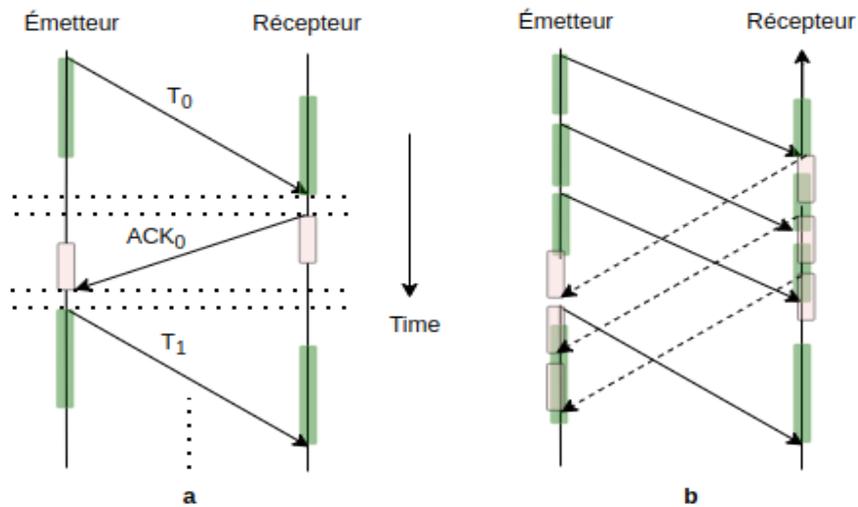


Fig. 4.1 Transmission avec arrêt et attente vs Transmission continue.

4.3.4 Modes d'exploitation d'une liaison de données

Il existe plusieurs modes d'exploitation d'une liaison de données qui se diffèrent selon les caractéristiques du circuit de données à savoir, le mode simplex, semi-duplex, full-duplex.

- Le mode simplex : dans ce mode, l'échange de données s'effectue dans un sens unique.
- Le mode semi-duplex : ce mode appelé aussi half-duplex ou à l'alternat, permet d'exploiter la liaison de données dans les deux sens mais alternativement (les transmissions simultanées engendrent des collisions).
- Le mode full-duplex : dit aussi duplex intégral, permet aux stations d'émettre simultanément et d'exploiter la liaison sans contrainte.

4.3.5 Concepts de base utilisés par les protocoles de liaison

4.3.5.1 Contrôle de flux

Le mécanisme de contrôle de flux est utilisé généralement dans le cas où le rythme d'émission des trames d'information par une machine émettrice dépasse le rythme de leurs traitements par celle réceptrice, et que cette dernière ne dispose plus de capacité mémoire pour en stocker les nouvelles arrivées en débordement [8]. Un exemple de transmission sans contrôle de flux (saturation de mémoire) est représenté dans la figure 4.2.

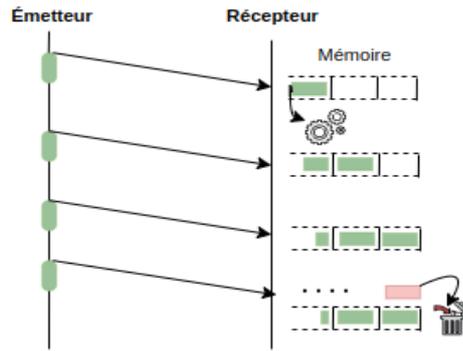


Fig. 4.2 Transmission sans contrôle de flux sur un circuit de données parfait

Afin d'éviter les problèmes de saturation et de perte de paquets, le mécanisme de contrôle de flux utilise deux trames de **supervision** (sans informations utiles), RR (Receiver Ready) et RNR (Receiver Not Ready) servant qu'à la gestion de liaison. Ces trames sont exploitées par les protocoles de liaison ainsi : après chaque réception, la machine réceptrice envoie la trame RR si elle est prête à accepter d'autres trames ou une trame RNR si sa capacité ne lui permet pas. Cependant, elle envoie une trame RR dès qu'elle devienne prête à accepter de nouvelles trames (voir figure 4.3).

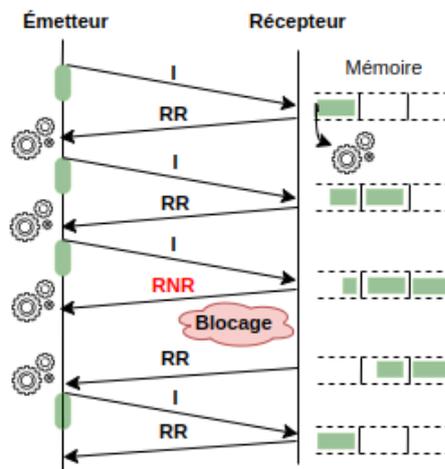


Fig. 4.3 Transmission avec contrôle de flux

4.3.5.2 Gestion des acquittements

L'une des stratégies de gestion des acquittements utilisée dans les protocoles de liaison de données est la stratégie d'acquiescement positif. En se basant sur cette stratégie le récepteur :

- En cas de réception d'une trame correcte, il répond avec un acquiescement positif (RR) ou négatif (RNR) selon l'état de sa mémoire.
- Dans le cas contraire (réception d'une trame erronée), il ne fait rien.

Le principe de gestion des trames est le suivant : l'émetteur arme un temporisateur pour chaque trame émise dont la durée est équivalente au temps d'attente maximale de l'acquiescement du récepteur. Si ce dernier ne répond pas, ou si sa réponse est brouillée, à la fin de cette durée, l'émetteur réémet la trame et incrémente le compteur de retransmission. Si ce compteur dépasse un seuil autorisé, on considère qu'un incident grave s'est produit et que la liaison de données est rompue.

4.3.5.3 Numérotation des trames d'information

Le problème de la stratégie précédente réside dans son incapacité à détecter la duplication de trames provoquée notamment en cas de perte d'acquittement. La solution à ce problème est d'introduire un mécanisme de numérotation pour distinguer la duplication des trames.

La numérotation des trames est placée dans un champ supplémentaire dans l'en-tête de la trame. Cette numérotation permet au récepteur de vérifier si une trame quelconque est bien en séquence afin de la faire délivrer à l'utilisateur.

Admettons que $N(S)$ est une variable donnant le numéro de la trame. Il peut prendre les valeurs (en modulo M) 2, 8 ou 128.

Le processus fonctionne de la façon suivante : l'émetteur (tout comme le récepteur) possède un compteur interne $V(S)$ donnant le numéro de la prochaine trame à émettre. Il émet cette trame en copiant $V(S)$ dans le champ $N(S)$, puis il incrémente $V(S)$. Pour toute répétition d'une trame d'information, il émet la trame sans modifier son numéro d'ordre.

4.3.5.4 Fenêtre d'anticipation

La notion de fenêtre permet à l'émetteur de faire plusieurs émissions successives sans attendre l'ACK des messages précédents. Le nombre de trames successives qu'on peut émettre sans réception d'acquittement est limité par une valeur notée k , appelée fenêtre. En effet, cette technique augmente l'efficacité des échanges grâce au fait qu'une seule trame de supervision permet d'acquitter un ensemble de trames qui se suivent sans erreur.

Le principe de fonctionnement est le suivant : à la réception d'une trame, le récepteur enregistre son numéro $N(S)$, l'incrémente de 1, le mémorise dans une variable interne $V(R)$ puis place cette valeur dans le champ $N(R)$ de la trame de supervision qu'il renvoie à l'émetteur (voir figure 4.4).

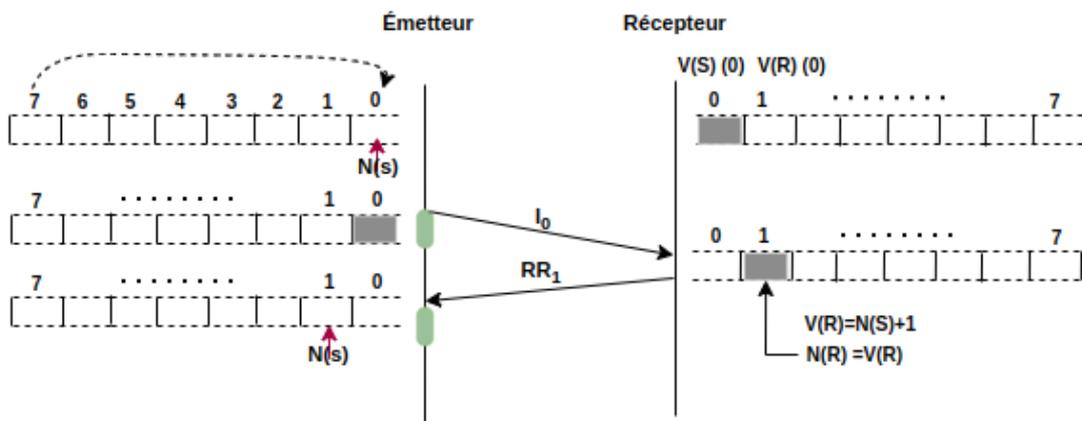


Fig. 4.4 Transmission avec contrôle de flux

Afin d'éviter certains problèmes liés à la réception retardée des acquittements, les trames d'acquittement (supervision) sont obligées de préciser les numéros des trames d'information qu'elles acquittent. Un scénario d'échange pour un protocole à fenêtre d'anticipation de taille 2 est illustrés à la figure 4.5.

Remarque : La taille de la fenêtre d'anticipation doit être gardée strictement inférieure au numéro de séquence des trames afin d'éviter la possibilité de recevoir deux trames successives portant le même indice.

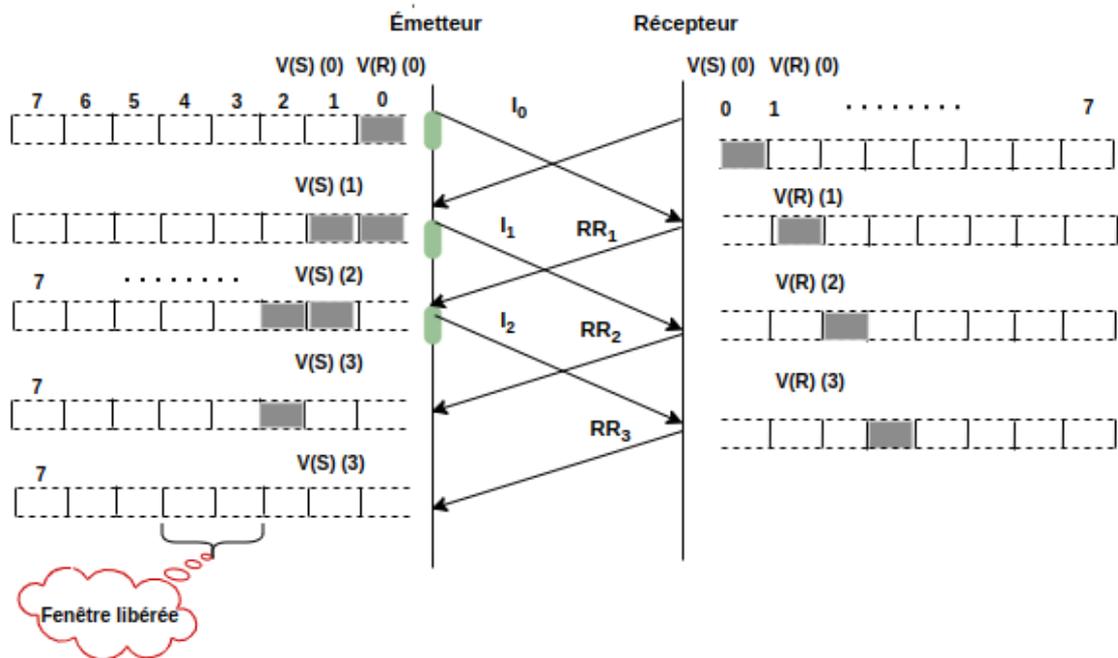


Fig. 4.5 Exemple d'échange pour un protocole à fenêtre d'anticipation de taille 2.

Enfin, en cas de réception d'une trame d'information dont le numéro de séquence ne correspond pas au $N(R)$ attendu, cette trame ne sera pas prise en compte et deux stratégies de retransmission sont envisageables :

- **Retransmission systématique (GO-BACK-N)** : Elle permet de reprendre la retransmission de toutes les trames à partir de la trame erronée. Cette stratégie est initiée dès qu'une rupture de séquence est détectée. Le récepteur dans ce cas demande la reprise d'émission à travers l'envoi d'une trame de supervision appelée **REJ (Reject)** dont le numéro $N(R)$ précise le numéro de la trame à partir duquel la retransmission doit être effectuée.
- **Retransmission sélective (Selective Reject)** : Cette stratégie ne réémet que la trame erronée. Elle utilise une trame de supervision de type **SREJ (Selective Reject)**

4.3.5.5 Piggy-Backing

Afin d'améliorer l'efficacité d'une liaison de données, les trames d'information peuvent véhiculer à la fois les informations à émettre et les acquittements des trames reçues précédemment. En effet, en plus de numéro de séquence $N(S)$, les trames d'information possèdent un numéro $N(R)$ acquittant les trames émises dans le sens opposé. Ce mécanisme est appelé piggy-backing et il est appliqué souvent dans les échanges bidirectionnels. Cependant, lorsqu'une station n'a pas de trame d'information à émettre, elle peut toujours utiliser des trames d'acquittement (RR , RNR ou REJ selon l'état de la réception) pour acquitter le trafic qu'elle reçoit. La figure 4.6 montre un échange de données en mode full duplex avec piggy-backing [8].

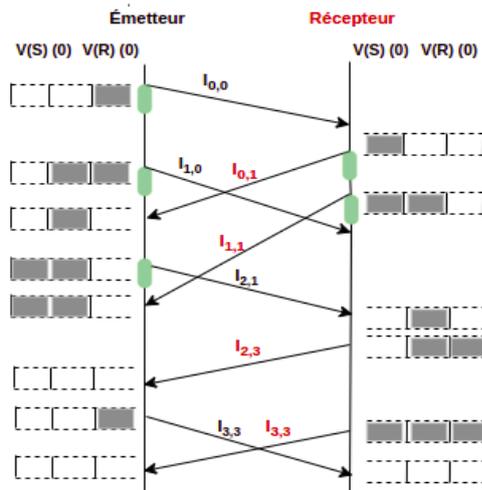


Fig. 4.6 Scénario d'un échange full duplex avec piggy-backing.

4.3.5.6 Gestion de liaison

Les contrôleurs de communication (CC) sont des éléments des ETTD qui sont reliés aux circuits de données (voir figure 3.5). Désormais, ils sont réalisés au niveau des cartes réseaux dans la technologie des réseaux locaux. Un CC est utilisé pour diverses raisons, notamment:

- L'ouverture de la liaison.
- La fermeture de la liaison.
- Le contrôle de l'échange de trames.

Le fonctionnement du contrôleur de communication dépend du protocole de liaison de données utilisé. Il existe énormément de protocoles de liaison de données, notamment : HDLC (High level Data Link Control), PPP (Point to Point Protocol), Ethernet / IEEE802.3, FDDI IEEE802.4, Token Ring IEEE802.5, etc [9].

4.4 Techniques d'accès au support

Dans les liaisons multipoints (les réseaux locaux tels que Token Ring, Ethernet, ATM, etc.), le lien de communication est partagé entre plus de deux appareils. Cependant, une seule machine peut y accéder à un instant donné pour éviter toutes sortes de collision de trames. De ce fait, l'accès au support doit être accordé selon des techniques d'accès bien déterminées qui sont regroupées en deux grandes familles : les méthodes d'accès aléatoire et les méthodes d'accès déterministes.

4.4.1 Méthode d'accès aléatoire

Dans ce type de technique d'accès, les appareils transmettent leurs données dès que celles-ci sont prêtes à être envoyées.

4.4.1.1 Méthode d'accès Aloha

C'est une méthode très ancienne qui appartient à ce mode d'accès. Elle consiste à envoyer un message, sans s'occuper de ce que font les autres équipements. En cas de collision, le message est retransmis au bout d'un temps aléatoire [10].

4.4.1.2 Méthode d'accès aléatoire CSMA (Carrier Sense Multiple Access)

Il s'agit d'une méthode d'accès aléatoire par laquelle un périphérique peut essayer d'accéder au support chaque fois qu'il veut envoyer une trame. Pour faire, il se met à l'écoute du canal de transmission (**l'écoute de la porteuse**), s'assurer de sa disponibilité avant de commencer la transmission. La technique CSMA/CD est l'une des variantes de cette technique d'accès.

Méthode d'accès CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Il s'agit d'une méthode d'écoute avec détection des collisions. Elle fonctionne ainsi : après le début de chaque émission, les équipements continuent d'écouter le support pendant une courte durée équivalente au temps de propagation aller et retour entre les deux stations les plus éloignées. Si une collision est détectée, ils arrêtent d'émettre au bout d'un court laps de temps. Après quoi ils attendent un délai relatif au nombre d'essai, pour tenter à nouveau d'envoyer leurs propres trames. Le nombre d'essais est limité à 16 tentatives après lesquelles les équipements abandonnent leurs transmissions. Le diagramme 4.7 donne plus de détails à cette technique [11].

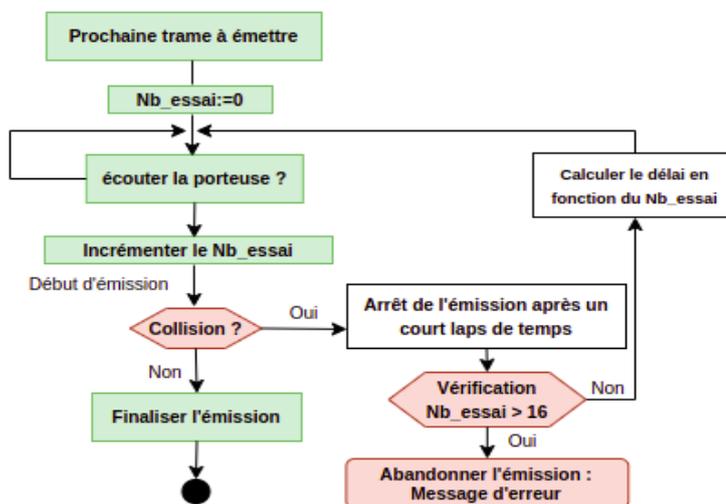


Fig. 4.7 Méthode d'accès CSMA/CD.

Remarque : malheureusement, le temps nécessaire pour émettre une trame avec cette technique ne peut être garanti.

4.4.2 Méthode d'accès déterministe

Ce mode d'accès repose sur l'utilisation d'un **jeton** qui transite dans le réseau d'une machine à l'autre. La machine qui le possède est autorisée à émettre sur le canal. Une fois sa transmission achevée, elle le transmet à la machine voisine.

Il existe différentes variantes de cette technique :

4.4.2.1 Méthode d'accès au support sur une topologie en anneau

Dans un réseau de topologie en anneau, les stations accèdent au support de transmission d'une façon successive grâce à un mécanisme de jeton (Token) circulant sur l'anneau.

Chaque équipement opérationnel doit participer à la réception et le passage du jeton même s'il n'a pas de trame d'information à envoyer (ou s'il n'a pas le droit pour émettre).

L'équipement émetteur (possesseur du jeton) qui a une trame à émettre, procède à son émission immédiatement après avoir armé un temporisateur. Une fois la transmission de cette trame est terminée, il passe à la transmission de la trame suivante si le temporisateur lui permet. Si ce n'est pas le cas, l'équipement doit passer le jeton à la machine suivante. Il y a un seul sens de rotation de l'anneau, l'équipement suivant est le premier équipement opérationnel, physiquement relié, c'est pourquoi le jeton utilisé dans cette technique est non adressé (voir figure 4.8).

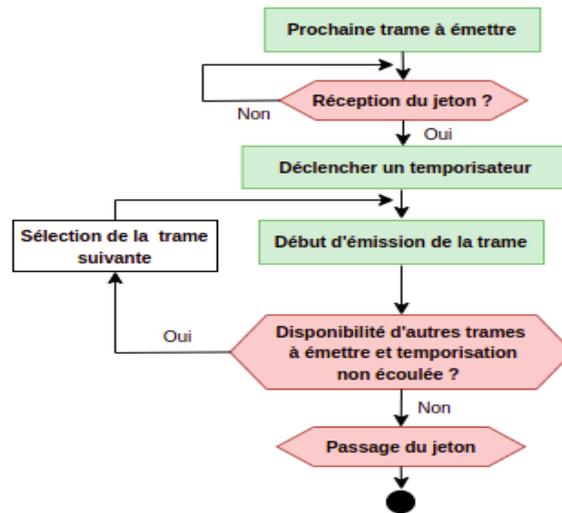


Fig. 4.8 Méthode d'accès avec jeton.

Les constructeurs ont estimé qu'un délai d'émission équivalant à 10 ms est approprié pour gérer l'accès équitablement [12].