Haute Ecole Spécialisée
de Suisse Occidentale

HEIG-VD – IICT

Jürgen Ehrensberger

Version 1.3. Janvier 2005

Chapitre 5
Réseaux Locaux

1 But du chapitre

Ce chapitre présente les technologies les plus importantes qui sont actuellement utilisées dans les réseaux locaux (LAN). Après une introduction dans les réseaux locaux, qui se réfère au modèle OSI, les technologies *Ethernet*, *Token Ring* et *Wireless LAN* sont décrites en détail.

Ce chapitre vous mettra en mesure de

- Connaître la situation des normes LAN dans la hiérarchie OSI (LLC, MAC)
- Connaître les méthodes d'accès aux médias
    - Savoir expliquer en détail le mécanisme CSMA
    - Savoir expliquer en détail le fonctionnement du protocole MAC des réseaux Ethernet
- Connaître les différentes variantes d'Ethernet ainsi que leurs supports physiques et les contraintes respectives
- Choisir une configuration appropriée d'un réseau Ethernet en fonction du nombre de stations à connecter, des services à offrir et du trafic prévu
- Savoir décrire le fonctionnement d'un réseau Token Ring
- Connaître les méthodes d'interconnexion de réseaux locaux (ponts)
- Connaître les fonctionnalités d'un pont transparent (filtrage, protocole de l'arbre recouvrant)
- Savoir expliquer le fonctionnement du protocole de l'arbre recouvrant
- Connaître le fonctionnement des VLANs
- Connaître les différentes normes de réseaux locaux sans fil
- Connaître les risques de sécurité des réseaux WLAN et les normes respectives

2 Introduction

Un réseau local (LAN, *Local Area Network*) a un débit de transmission élevé et couvre une zone géographique restreinte. Il est typiquement utilisé pour connecter les stations, PCs, imprimantes et serveurs d'une entreprise.

2.1 Les protocoles LAN et le modèle de référence OSI

Les protocoles utilisés dans les réseaux locaux fonctionnent aux deux couches inférieures du modèle OSI, entre la coche physique et la couche liaison de données. La Figure 1 positionne les protocoles LAN les plus importantes dans la hiérarchie OSI.

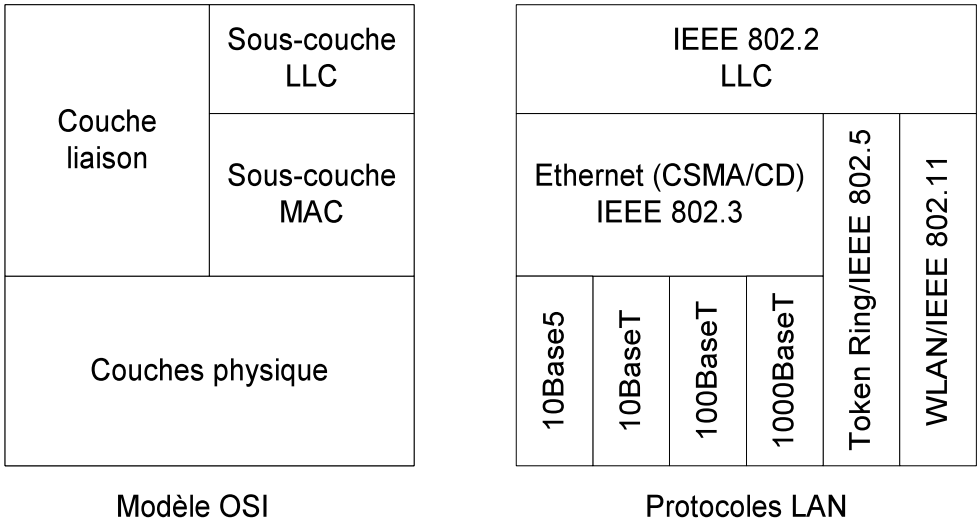


Figure 1: Relation entre les protocoles LAN et le modèle OSI

La figure montre que la couche 2 du modèle OSI est partagée en deux sous-couches, à savoir la sous-couche MAC (*Medium Access Control*) et la sous-couche LLC (*Logical Link Control*). Alors que la sous-couche LLC s'occupe de résoudre les problèmes de communication spécifique au niveau ligne indépendamment de la technologie sous-jacente, la sous-couche MAC, elle, gère l'accès au média et dépend du support physique utilisé.

Pour les différents médias, de sous-couches MAC ont été définies, en particulier dans le contexte du projet 802 des normes LAN/MAN de l'IEEE (*Institute of Electrical and Electronics Engineers*). Les groupes de travail de ce projet ainsi que les normes en vigueur sont :

Groupe 802.1 : Protocoles de couches supérieures dans les réseaux locaux
Architecture de réseaux 802 LAN/MAN et leur interconnexion

- Norme **802.1D** : ponts LAN (Interconnexion de réseaux LAN)
- Norme **802.1Q** : réseaux LAN virtuels.
  Comprend la norme **802.1p** (classes de trafic et priorités dans les réseaux LAN)

Groupe 802.2 : LLC

Groupe 802.3 : Ethernet

Développement de normes pour les réseaux LAN utilisant CSMA/CD.

- Norme **802.3** : Ethernet.
  Comprend les normes pour 10 Mb/s Ethernet, FastEthernet, Gigabit-Ethernet et 10Gb/s Ethernet.

Groupe 802.5 : Token Ring

Groupe 802.11: Réseaux locaux sans fil

- Norme **802.11a** : Réseaux sans fil jusqu'à 54 Mb/s dans la bande de 5 GHz
- Norme **802.11b** : Réseaux sans fil jusqu'à 11 Mb/s dans la bande de 2.4 GHz
- Norme **802.11e** : Qualité de service dans les réseaux 802.11
- Norme **802.11i** : Sécurité
- Norme **802.11g** : Extension de 802.11b pour un débit de 54Mb/s

Groupe 802.12 : *Demand Priority*

- Norme 802.12a : 100VG-AnyLAN

Groupe 802.15 : Réseaux PAN (*Personal Area Networks*) sans fil

- Norme 802.15.1 : Bluetooth

3 Couche Liaison

Les réseaux locaux ont des particularités assez différentes des réseaux étendus (WAN). Ils sont multipoint, c'est-à-dire que toutes les stations peuvent être atteintes à partir d'un coupleur. Le taux d'erreur bit en ligne est généralement très faible puisque la distance à parcourir entre les divers points est faible, de l'ordre de grandeur de 10^{-10}. De ce fait, on ne peut plus stipuler que la couche 2 doit rendre le taux d'erreur encore plus petit.

La prise en compte des caractéristiques des réseaux locaux a poussé l'ISO à normaliser un protocole de liaison spécifique pour les réseaux locaux. Le travail a, en grande partie, été effectué par le groupe 802.2 de l'IEEE. La norme correspondante reprise par l'ISO porte la valeur 8802.2. C'est la norme LLC (*Logical Link Control*).

3.1 LLC

Comme déjà mentionné, la sous-couche LLC effectue les tâches de la couche liaison du modèle OSI qui sont indépendantes de la technologie sous-jacente.

En réalité, il n'y a pas une norme LLC, mais trois : LLC 1, LLC 2 et LLC 3, adaptées chacune à des modes de fonctionnement différents.

LLC 1 (*unacknowledged connectionless service*). Ce protocole est souvent appelé tout simplement LLC. Il effectue des transmissions de blocs isolés, sans connexion (Figure 2a). La reprise sur erreur et le contrôle du séquencement sont laissés aux couches supérieures.
Les réseaux Ethernet utilisent en général le service de ce type.
Lors de l'élaboration de la norme LLC 1, le très faible taux d'erreur résiduelle au sommet de la couche 1 a été pris en compte. Il était inutile de mettre en œuvre une technique de reprise sur erreur. Le protocole LLC 1 est en conséquence assez simple et comporte peu de fonctionnalités. Cependant, une zone de contrôle d'erreur a été introduite dans la trame afin de vérifier que les erreurs sont bien en nombre négligeable. Lorsqu'une trame en erreur est détectée, elle est détruite pour éviter que des informations erronées soient utilisées. Le taux d'erreur résiduelle peut ne plus être négligeable après ces destructions. Puisque le protocole LLC 1 n'a pas la possibilité d'effectuer les reprises nécessaires, un niveau supérieur de l'architecture doit s'en occuper. Comme nous l'avons vu au chapitre 2, c'est le protocole TCP qui effectue la reprise.

LLC 2 (*connection mode service*). La norme LLC 2 provient d'une constatation simple : si le nombre d'erreur en ligne n'est pas négligeable, plutôt que repousser le problème de la correction à un niveau supérieur, il est préférable d'effectuer directement la reprise sur erreur au niveau liaison (couche 2). Pour sécuriser l'acheminement des données, la norme LLC 2 spécifie un protocole de liaison en mode avec connexion et l'utilisation d'acquittements (Figure 2b).

LLC 3 (*acknowledged connectionless service*). La norme LLC 3 est sans connexion mais avec acquittement du type « *envoyer et attendre* » (*stop-and-go*).
Une trame ne peut être envoyée qu'après la confirmation de réception de la trame précédente. Le récepteur peut décider s'il est utile de renvoyer une trame

erronée, donc sans acquittement.
Ce type d'opération est utilisé surtout dans les réseaux industriels lorsque l'ordinateur central interroge à tour de rôle les différents équipements périphériques disposant d'une mémoire limitée.

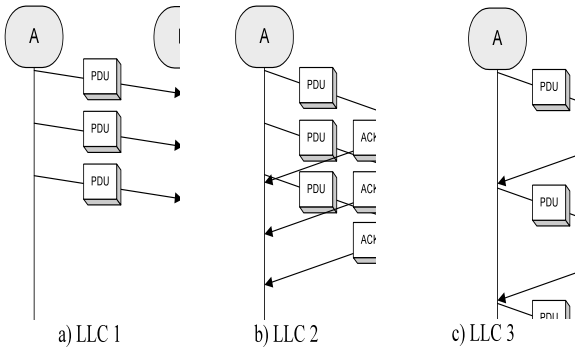


Figure 2: Fonctionnement des différents modes de LLC

Format des PDU LLC. Les différents types du protocole LLC utilisent le même format de PDU (*Protocol Data Unit*), montré dans la Figure 3.

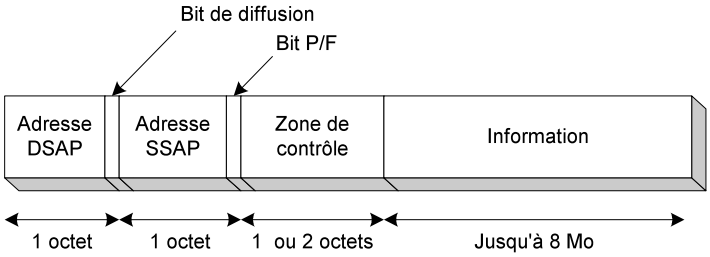


Figure 3: Format de PDU du protocole LLC

Il y a deux champs d'adresse, de la destination (DSAP) et de la source (SSAP), chacun sur 7 bits. Le bit supplémentaire du premier octet indique une adresse multipoint. Les adresses DSAP et SSAP sont utilisées par LLC pour identifier le type de protocole auquel se rapportent les données dans le champ « information ».

Le dernier bit du deuxième octet (bit P/F) indique si la trame doit être interprétée comme commande ou comme réponse.

Le contenu du champ de contrôle dépend du type de la PDU. Il est code sur un ou deux octets.

Le dernier champ contient la PDU de la couche supérieure (donc les données de la couche réseau à transmettre).

Pour la transmission, les LLC-PDUs sont passées à la sous-couche MAC qui les encapsule dans une trame MAC en ajoutant d'en-têtes et d'en-queues, comme montré dans la Figure 4.

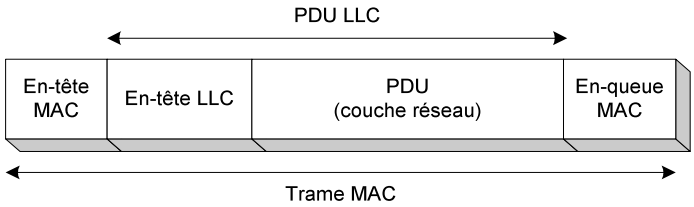


Figure 4: Encapsulation de la PDU LLC dans une trame MAC

3.2 MAC

Dans les réseaux locaux les transmissions s'effectuent en générale par diffusion sur un réseau multipoint. Dans un tel réseau, tous les abonnés ont la possibilité d'émettre et de recevoir. Le problème majeur consiste à déterminer qui, à un instant donné, a le droit d'émettre. On a conçu de nombreux protocoles ayant pour but de résoudre le problème d'accès à un média partagé. Ces protocoles sont regroupés dans la sous-couche MAC (*Medium Access Control*). Cette sous-couche joue un rôle très important dans les réseaux LAN, et plus particulièrement dans ceux dont le fonctionnement repose sur le principe de l'accès multiple.

Plusieurs méthodes de partage d'un canal sont possibles.

Partage statique. Le partage est dit *statique* lorsque chaque station dispose en permanence de l'accès à une partie du canal, sans interférence avec les communications échangées par les autres stations. Le partage statique peut être assuré, par exemple, par division du canal en bandes de fréquences (*multiplexage en fréquence*) ou par *multiplexage temporel.* Dans ce dernier cas, chaque station dispose d'une tranche de temps fixe pour émettre ses messages. Le partage statique d'une voie revient donc à réaliser un réseau où chaque émetteur dispose d'une ligne fixe sur laquelle sont branchés tous les récepteurs des autres stations.

Partage dynamique. Le partage statique des voies convient mal au trafic de données car celui-ci s'écoule en général par salves (*bursts*) dont l'arrivée peut être considérée comme aléatoire et qui correspond à un débit instantané très élevé avec une valeur moyenne faible. Ceci conduit à partager les voies de manière *dynamique* en transmettant les données par paquets et en allouant le canal aux utilisateurs soit par *élection*, soit par *contention*.

- La première méthode (élection) consiste à donner la parole à chaque station à tour de rôle selon un cycle, qui peut être déterminé par la topologie du réseau (réseaux à jeton en anneau) ou selon un ordre préétabli (réseau à jeton avec une topologie en bus)
- La deuxième méthode, la méthode de contention, consiste à permettre à chacune des stations, sans concertation aucune, de prendre possession du média pour transmettre des données. Ceci peut provoquer des conflits lorsque plusieurs stations initient des transmissions simultanées. Dans ce cas là, chaque station ayant remarqué la collision devra alors mettre en œuvre une procédure (appelée *résolution de collision*) aboutissant au renoncement ou à la conquête exclusive de la ressource.

Les réseaux Ethernet utilisent une méthode de compétition appelée CSMA. Cette méthode est décrite à la Section 1. La méthode d'élection, utilisée par les réseaux Token Ring, est décrite dans la Section 5.

4 Ethernet

Historique

Robert Metcalfe, David Boggs et d'autres chercheurs de Xerox Corporation développèrent un réseau local fondé sur des mécanismes de détection de porteuse. Ce réseau possédait une longueur d'un kilomètre, supportait cent stations et transmettait les données à 2,94 Mb/s. Ce système a été appelé Ethernet du nom de cette substance impalpable, l'éther, imaginée au XVIIIe siècle pour expliquer la propagation des ondes électromagnétiques (le terme "net" rappelle, lui, qu'il s'agit d'un réseau). La première conception d'un réseau Ethernet est montrée dans la Figure 5

Ethernet a été proposé comme standard par Digital Equipment Corporation, Intel et Xerox. Le premier standard a été publié en septembre 1981 et a été appelé DIX 1.0. DIX signifie Digital, Intel et Xerox. DIX 1.0 a été suivi par DIX 2.0, publié en novembre 1982. Le standard DIX 2.0 est aussi appelé Ethernet II.

Pendant ce temps, l'IEEE a continué la standardisation des réseaux locaux, commencée par le projet 802. Digital, Intel et Xerox proposaient l'adoption d'Ethernet comme standard. IBM proposa Token Ring (basé sur des prototypes construits dans les laboratoires d'IBM à Zurich) comme standard. La proposition Ethernet devint le standard IEEE 802.3, et Token Ring devint le standard 802.5.

Du fait de la nature même du comité, le standard IEEE 802.3 n'est pas tout à fait identique à celui d'Ethernet. Il existe même d'importantes différences. Bien que les standards 802.3 et Ethernet soient **incompatibles**, le terme *Ethernet* est utilisé dans les réseaux TCP/IP pour désigner les réseaux 802.3. Nous adoptons l'usage commun et utilisons le terme Ethernet pour les deux standards, en notant les différences quand cela est nécessaire.

Ethernet est aussi connu sous d'autres noms. En 1989, l'ISO l'adopta comme standard ISO/IEC 8802-3.

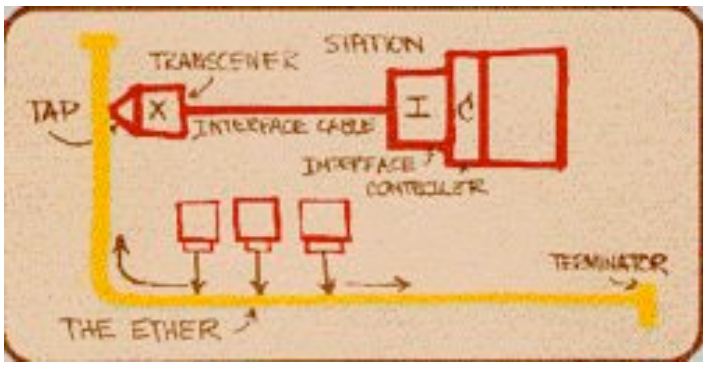


Figure 5: Première conception d'un réseau Ethernet

Le mot Ethernet est synonyme de réseaux locaux. Conçu initialement pour un support physique partagé, la grande révolution du monde Ethernet a été de passer en mode commuté et non plus partagé, comme nous allons le voir.

Les modes partagé et commuté. Ethernet fonctionne selon deux modes très différents mais totalement compatibles, le mode *partagé* et le mode *commuté*, qui permettent tous deux de transporter des trames Ethernet. Le mode partagé indique bien que le support physique est partagé entre les terminaux munis de carte Ethernet. Dans ce mode, deux stations qui émettraient en même temps verraient leurs signaux entrer en collision. Dans le mode commuté, les terminaux sont connectés à un commutateur, et il ne peut y avoir de collision des transmissions des terminaux puisque le terminal est seul sur la liaison connectée au commutateur. Le commutateur émet vers la station sur la même liaison soit en full-duplex, c'est-à-dire en parallèle mais dans l'autre sens, soit en half-duplex, ce qui peut provoquer des collisions entre le terminal et le commutateur.

La Figure 6 illustre les deux techniques avec cinq stations terminales.

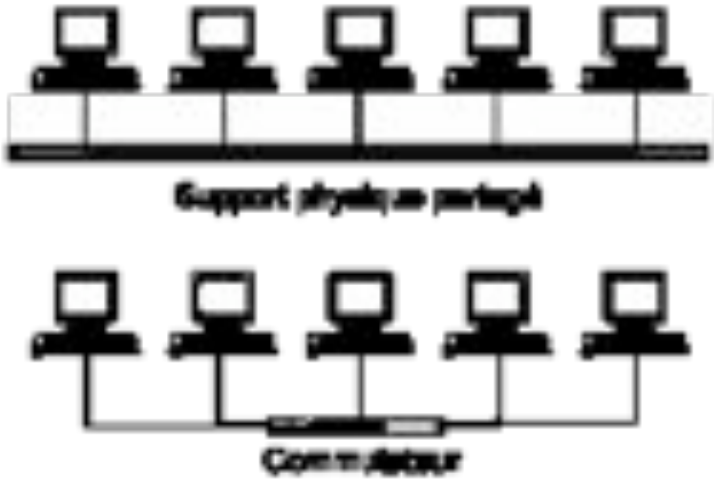


Figure 6: Comparaison des techniques partagées et commutées

Les avantages et les inconvénients des deux techniques sont nombreux, notamment les suivants :

- Il y a moins de collision ou plus de collisions du tout en mode commuté, mais les trames doivent être mémorisées dans les commutateurs, ce qui demande un contrôle de flux.
- Pour connecter une station en commutation, il faut deux interfaces et un commutateur, tandis que pour connecter une station en mode partagé, un seul coupleur est suffisant. La technique partagée est donc moins chère à mettre en œuvre.
- La technique commutée autorise des liaisons sans contraintes de distance, tandis que la méthode partagée s'accompagne d'une limitation forte de la distance pour résoudre le problème du partage du support physique.

Nous commençons par l’étude du mode partagé.

4.1 Accès aléatoire à un média partagé

Historique

Vers la fin des années 70, l'Université de Hawaii a développé et utilisé un système de communication par radio (**ALOHA**) afin de connecter les différentes îles d'Hawaii. Le protocole utilisé permettait à chaque station connectée d'émettre à tout moment ce qui conduisait à des collisions de transmissions dans le canal radio partagé. Le protocole ALOHA est l'origine des protocoles MAC modernes utilisant la méthode CSMA (*Carrier Sense Multiple Access*).

Un réseau ALOHA peut être considéré comme un ordinateur central et un certain nombre de terminaux reliés entre eux par un canal radio commun.

Si un terminal désire envoyer de l'information à une autre station, il regroupe les données à envoyer dans un paquet qui contient en outre l'adresse de la station destinataire. Le terminal émet ensuite le paquet sur le canal radio, sans se préoccuper de savoir si le canal est libre ou non. Le terminal attend ensuite pendant un délai déterminé un message d'acquittement en provenance du destinataire. Si le message d'acquittement arrive dans les délais prescrits, la transmission s'est effectuée correctement et la transaction est terminée.

S'il y avait collision, c'est-à-dire superposition des signaux de deux ou plusieurs utilisateurs, les signaux deviennent indéchiffrables et sont perdus. Dans ce cas-là, les émetteurs ne recevront pas d'acquittements et devront répéter leurs transmissions. Pour éviter que les mêmes trames n'entrent en collision à nouveau, chaque émetteur doit observer un temps d'attente aléatoire avant de retransmettre.

Il faut remarquer que même si le premier bit d'une trame recouvre le dernier bit d'une autre, les deux trames seront détruites et devront être retransmises.

4.1.1 Performances du protocole ALOHA

Il est intuitivement clair que lorsqu'il y a beaucoup d'utilisateur dans un réseau ALOHA il y aura souvent des collisions de transmission, ce qui diminue le temps effectif pendant lequel des données peuvent être transmises correctement. Nous allons analyser de manière mathématique le comportement d'un réseau ALOHA.

Pour cela nous faisons les hypothèses suivantes :

- Nous supposons un nombre très grand d'utilisateurs qui génèrent des trames avec une certaine fréquence. Le nombre de trames par seconde générées par tous les utilisateurs soit donné par λ_{gen}. L'hypothèse d'un grand nombre d'utilisateur est nécessaire pour éviter que la fréquence λ_{gen} ne dépende du nombre d'utilisateurs en état d'attente avant une retransmission[1].

[1] Plus précisément nous supposons que les trames sont générées selon un processus de Poisson avec une intensité λ.

- Le canal de transmission ne présente pas d'erreurs de transmission. La seule cause de perte de trame est une collision de transmissions.
- Nous négligeons le temps de propagation du signal entre les stations.

Ce qui nous intéresse est le rapport entre le trafic transmis avec succès (donc sans collision) et le trafic total offert au canal (donc toutes les tentatives de transmission)

Le trafic offert A du réseau est défini comme le produit de la fréquence de toutes les transmissions et la durée moyenne d'une transmission :

$$A = \lambda_{tot} \cdot \tau .$$

La fréquence λ des transmissions comprend les nouvelles trames générées par les utilisateurs et les retransmissions, donc

$$\lambda_{tot} = \lambda_{gen} + \lambda_{retr} .$$

Le trafic transmis avec succès est appelle trafic écoulé et dénoté par le symbole *Y*. Il est défini comme le produit de la fréquence de réception correcte d'une trame et la durée moyenne d'une trame :

$$Y = \lambda_{reçu} \cdot \tau .$$

Déterminons maintenant dans quelles conditions la trame représentée en grisé sur la Figure 7 sera transmise correctement, donc sans subir de collision. Si une station a transmit une trame dans l'intervalle compris ente t_0 et $t_0+\tau$ la fin de cette trame télescopera le début de la trame en grisé. En fait, le sort de la trame en grisé était déjà fixé avant que le premier de ses bits ne soit transmis, mais dans le protocole ALOHA les stations n'écoutent pas le canal avant de transmettre.

De même, toute trame transmise entre $t_0+\tau$ et $t_0+2\tau$ télescopera la trame en grisé. Cet intervalle de temps entre t_0 et $t_0+2\tau$ pendant lequel aucune autre station ne doit initier la transmission d'une trame est appelé période de vulnérabilité.

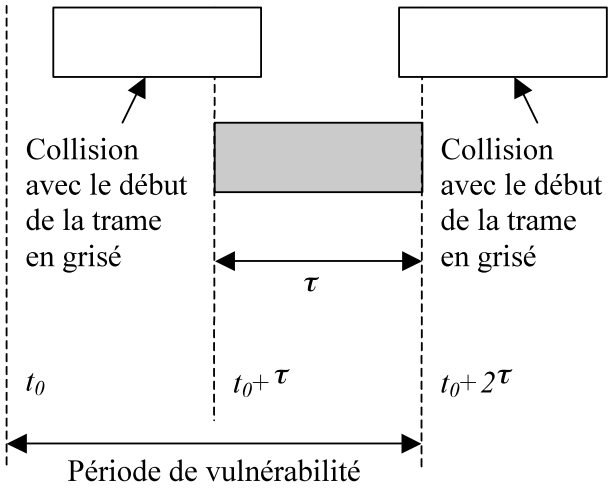


Figure 7: Période de vulnérabilité d'une trame dans ALOHA

Le trafic écoulé est la partie du trafic offert qui n'a pas subit de collision. Dénotons la probabilité de collision par P_0, donc

$$Y = P_0 \cdot A$$

Pour un trafic poissonnien avec fréquence λ la probabilité que k trames soient générées pendant un intervalle de temps t est donnée par la formule de la distribution de Poisson :

$$\Pr(k) = \frac{(\lambda t)^k e^{-\lambda t}}{k!}.$$

Ainsi nous pouvons déterminer P_0, donc la probabilité qu'aucune trame soit transmise pendant la période de vulnérabilité d'une trame :

$$P_0 = \frac{(2A)^0 e^{-2A}}{0!} = e^{-2A}$$

et finalement

$$Y = A \cdot P_0 = A \cdot e^{-2A}.$$

La relation entre le trafic offert A et le trafic écoulé Y est illustrée dans la Figure 8.

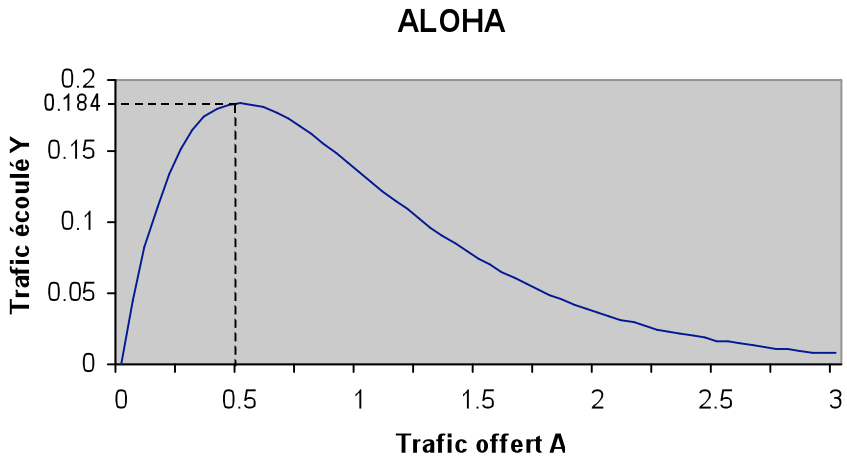


Figure 8: Relation entre le trafic offert et le trafic écoulé dans ALOHA

Pour un trafic offert très faible, il n'y a presque pas de collision, donc le trafic écoulé est très proche du trafic offert. Avec l'augmentation du trafic offert, des collisions se produisent plus souvent et l'écart entre le trafic offert et le trafic écoulé croît. Le trafic écoulé atteint le maximum de Y=0.184 pour un trafic offert de A=0.5. En d'autres termes, le mieux que l'on puisse espérer correspond à une occupation utile du canal de l'ordre de 18 %. Pour un trafic offert élevé, le canal est très souvent occupé par de trames en collision, qui ne contribuent pas au trafic écoulé. Ce résultat n'est pas très encouragent.

4.1.2 Le système ALOHA discrétisé (*slotted ALOHA*)

L'utilisation maximale très limitée du canal dans le système ALOHA a conduit à la recherche d'améliorations possibles. En 1972, une méthode a été publie qui permettait de doubler utilisation du système. La proposition consistait à diviser le temps en intervalles répétitifs (appelés slots) de durée constante, à savoir la durée d'une trame. Une station ne peut commencer la transmission d'une trame qu'au début d'un slot. Cette méthode nécessite une synchronisation des différentes stations. Une méthode pour établir cela serait d'utiliser une station qui émettrait. A intervalle de temps régulier, telle une horloge, un signal indiquant le début de chaque slot.

Dans slotted ALOHA, s'il y a collision, c'est sur l'ensemble du slot et non plus sur des parties de trames seulement. L'effet de cette discrétisation du temps et que la période de vulnérabilité est réduite à la durée de la transmission d'une trame, comme montré dans la Figure 9.

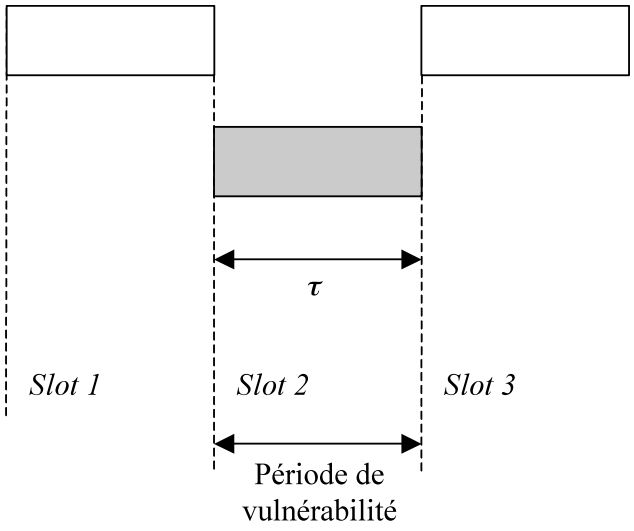


Figure 9: Période de vulnérabilité d'une trame dans *slotted ALOHA*

Le même calcul comme pour le système ALOHA pur, à la différence près d'une période de vulnérabilité de τ au lieu de 2τ, nous donne la relation entre le trafic écoulé Y et le trafic offert A dans slotted ALOHA :

$$Y_{\text{slotted}} = A \cdot e^{-A}.$$

La Figure 10 compare les deux systèmes d'ALOHA.

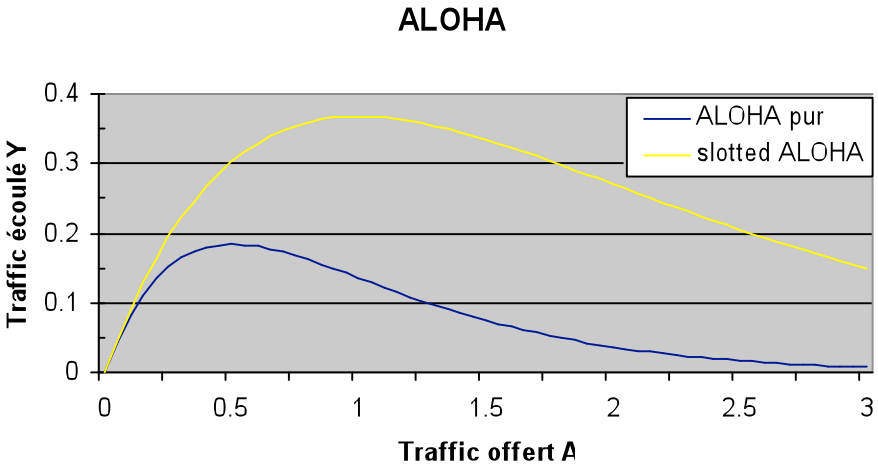


Figure 10: Comparaison d'ALOHA pur et slotted ALOHA

Le mieux qu'on puisse espérer d'ALOHA discrétisé se repartit comme suit :

- 36,8 % d'intervalles de temps non utilisés (=P_0),
- 36,8 % de transmission réussies (= trafic écoulé Y) et
- 26,4 % de collisions (= 1- P_0-Pr(1)).

En utilisant un trafic offert plus élevé, il est possible de réduire le nombre de slots non utilisés main on accroît exponentiellement le nombre de collisions.

Si plusieurs stations essaient de transmettre en même temps, leurs paquets entrent en collision et doivent être retransmis. Les paquets retransmis peuvent à leur tour faire l'objet d'une collision, ce qui nécessite une nouvelle retransmission. On conçoit donc que la transmission des paquets peut subir un retard important dans les cas extrêmes. Compte tenu de la nature statistique du protocole de communication, le retard subi par un paquet dans un réseau aléatoire est imprévisible.

Nous allons maintenant déterminer le retard moyen subi d'une trame à cause de collision en fonction du trafic offert. La probabilité qu'une trame n'ait pas de collision est $P_0 = e^{-A}$. La probabilité qu'elle y ait collision est $1 - P_0 = 1 - e^{-A}$. La probabilité pour que la transmission nécessite exactement *k* tentatives, c'est-à-dire *k-1* collisions suivies par une transmission réussie, est :

$$P_k = e^{-A}(1 - e^{-A})^{k-1}.$$

Le nombre moyen de transmissions *E* pour chaque trame est alors :

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-A}(1 - e^{-A})^{k-1} = e^{A}.$$

Nous avons vu dans la description d'ALOHA, qu'une station doit attendre un délai aléatoire après une collision avant de retransmettre la trame. Supposons qu'elle choisit avec la même probabilité une valeur *n* entre 1 et *N* telle qu'elle attend *nième* slot après la collision pour retransmettre la trame. Le délai moyen entre les transmissions est donc : $\frac{N+1}{2}\tau$. Le délai moyen pour une transmission réussi est donc donné par

$$D = (e^{A} - 1)\frac{N+1}{2}\tau + \tau.$$

La Figure 11 montre le délai moyen de transmission *D* en fonction du trafic offert pour *N*=4.

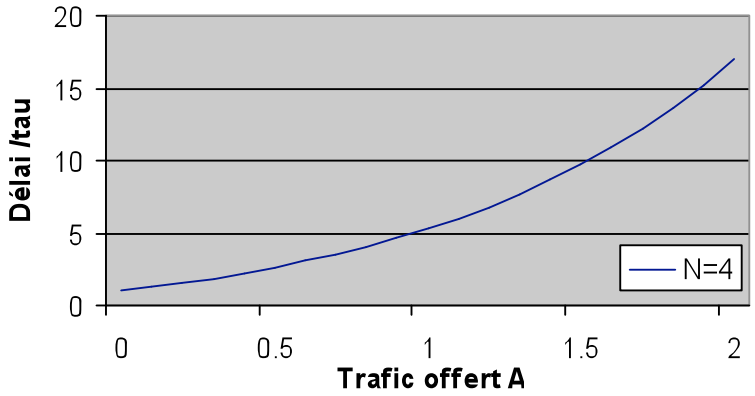


Figure 11: Délai de transmission à cause de retransmissions dans slotted ALOHA

4.1.3 CSMA

Dans un système ALOHA les stations transmettent sans contrainte, sans se soucier de ce que font les autres stations. En conséquence on observe de nombreuses collisions. Toutefois, avec les réseaux LAN une station peut s'enquérir de ce que font les autres stations et adapter alors son comportement.

Cette technique, plus connue sous le nom de CSMA (*Carrier Sense Multiple Access*), consiste à écouter le canal avant d'émettre. Si le coupleur détecte un signal sur la ligne, il diffère son émission à une date ultérieure. Cela réduit considérablement les risques de collision, sans toutefois les supprimer complètement. En effet, si, durant le temps de propagation entre le couple de stations les plus éloignées (période de vulnérabilité), une station ne détecte pas l'émission d'une trame d'une autre station, il peut y avoir superposition de signaux. De ce fait, il faut ré-émettre ultérieurement les trames perdues.

De nombreuses variantes de cette technique existent. Elles diffèrent par trois caractéristiques :

- La stratégie suivie par le coupleur après détection de l'état du canal.
- La manière dont les collisions sont détectées.
- La politique de retransmission des messages après collision.

Nous décrivons ci-après quelques-unes de ces variantes.

CSMA non persistant. La station écoute le canal lorsqu'une trame est prête à être envoyée, Si le canal est libre, la station émet. Dans le cas contraire, elle recommence le même processus après un délai aléatoire.

CSMA persistant (ou 1-persistant). De même que précédemment, une station prête à émettre écoute préalablement le canal et transmet s'il est libre. Si elle détecte l'occupation de la porteuse, elle continue à écouter jusqu'à ce que le canal soit libre et émet à ce moment là.
Cette technique permet de perdre moins de temps que dans le cas précédent, mais elle a l'inconvénient d'augmenter la probabilité de collision, puisque les trames qui s'accumulent pendant la période occupée sont toutes transmises en même temps.

CSMA p-persistant. Dans cette approche, l'algorithme est le même que précédemment, mais, lorsque le canal devient libre, la station émet avec la probabilité *p*. En d'autres termes, la station diffère son émission avec la probabilité *1-p*. Cet algorithme permet de réduire la probabilité de collision. En supposant que deux terminaux souhaitent émettre, la collision est inéluctable dans le cas de CSMA persistant. Avec ce nouvel algorithme, il y a une probabilité *1-p* que chaque terminal ne transmette pas et donc évite la collision. En revanche, il augmente le temps avant la transmission, puisqu'un terminal peut choisir de ne pas émettre, avec probabilité *1-p*, alors que le canal est libre.

Les diagrammes de flux des différentes variantes sont montrés dans Figure 12. Les performances sont comparées dans la Figure 13.

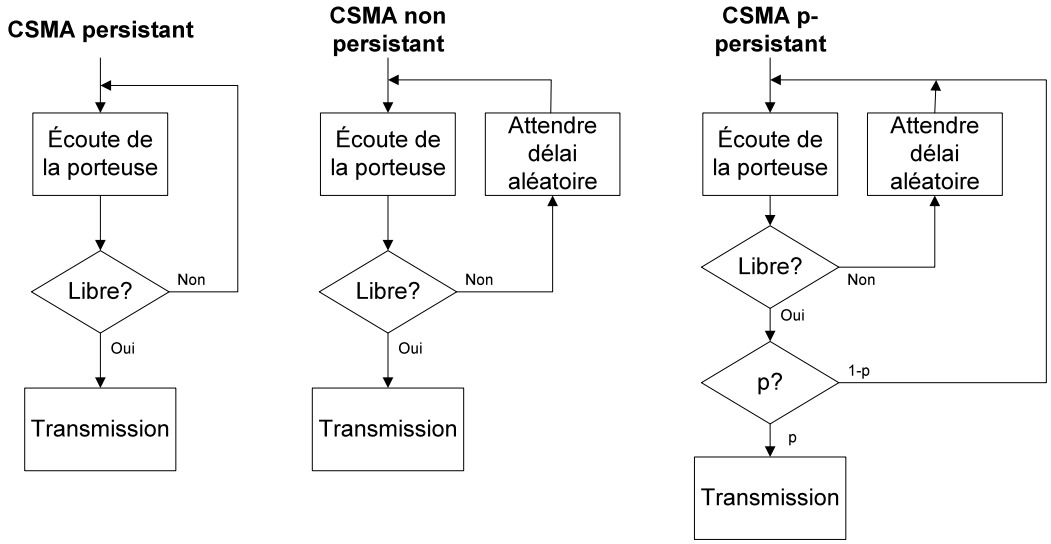


Figure 12: Diagrammes de flux des méthodes CSMA

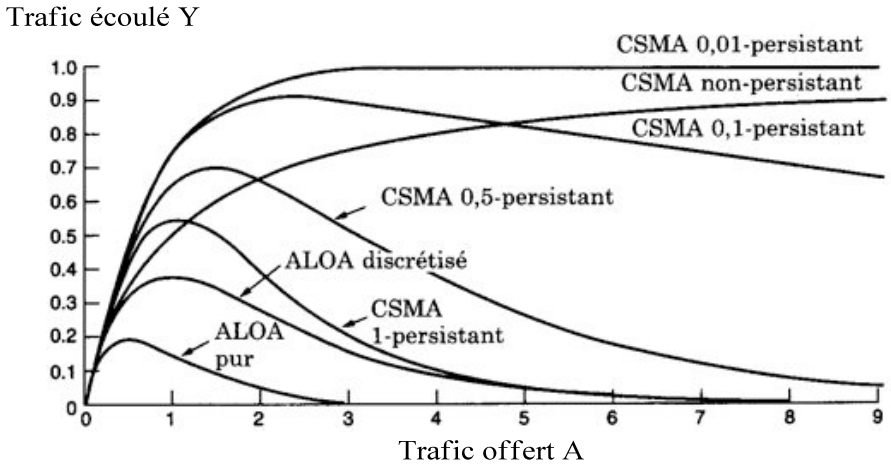


Figure 13: Comparaison des méthodes CSMA

4.2 La sous-couche MAC Ethernet

Les réseaux Ethernet ont initialement été conçus pour l'utilisation d'un câble coaxial partagé comme support physique. Le fonctionnement de la sous-couche MAC Ethernet et fortement orienté vers les caractéristiques de ce média. Il s'agit en fait d'une amélioration de la technique CSMA. Les stations écoutent en permanence le canal, même lorsqu'elles émettent, ce qui peut être réalisé de façon très simple sur un câble[2]. Lorsqu'une collision se produit, elle est détectée très tôt et les stations peuvent immédiatement arrêter la transmission. Cette méthode de contrôle d'accès au média s'appelle CSMA/CD (*Carrier Sense Multiple Access and Collision Detect*).

[2] Ceci n'est pas possible p.ex. dans une transmission radio où une station n'est pas capable d'écouter le canal lorsqu'elle transmet.

4.2.1 CSMA/CD

La propagation de une trame sur le média partagé est bidirectionnelle: une trame qui est envoyée par une station située au milieu du câble se propagera des deux côtés du câble.

Une station ne peut émettre que si elle ne détecte pas de message sur le canal. Celle-ci vérifie par **détection de porteuse** (*Carrier Sense*) que le média est libre, c'est-à-dire qu'aucune trame n'est en train de circuler. Trois cas peuvent se présenter:

1. La station émettrice est la seule qui veut émettre: La station détecte que le canal est libre et émet une trame. La trame se propage dans tout le réseau. Toutes les stations connectées sur le segment la voient, mais seul le destinataire la traite.

2. La station qui aimerait émettre détecte que le canal est occupé parce qu'une autre transmission est déjà en cours. La station attend donc son tour. Pour cela elle continue de surveiller la porteuse jusqu'à ce que le média soit libre (d'après la méthode 1-persistant). Lorsque le média est libre elle émet sa trame.

3. Deux stations aux extrémités du média veulent émettre en même temps: Chacune des stations avant d'émettre vérifie que le média est. Cela étant le cas, les deux stations émettent à peu près simultanément et provoquent une collision. Ceci est illustré dans la Figure 14.
   La collision se manifeste électriquement sur les câbles coaxiaux par une violation de la méthode de codage des bits. La collision est donc un phénomène parfaitement normal et inhérent au principe du protocole Ethernet. Seul un taux de collision trop élevé pendant un certain temps peut être anormal et être le symptôme d'un dysfonctionnement du réseau.

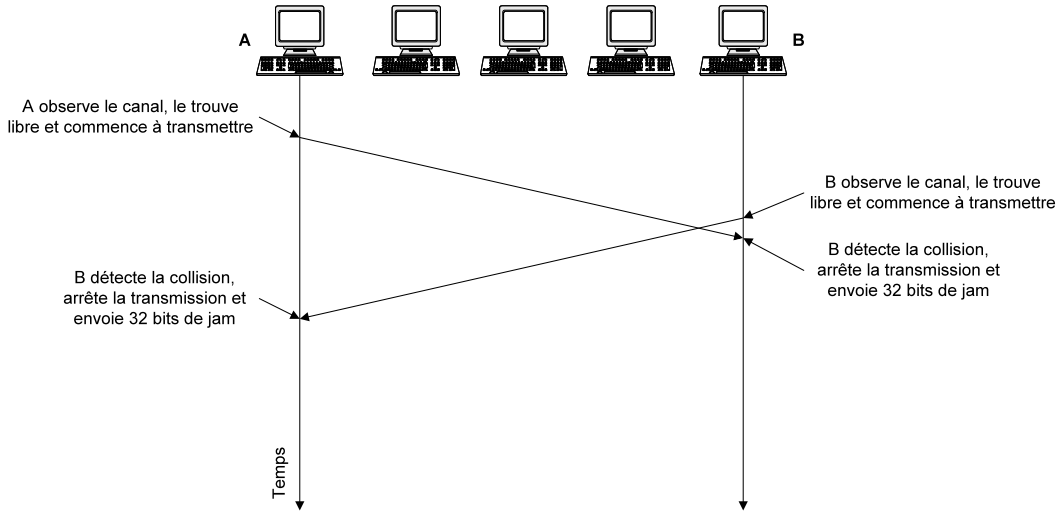


Figure 14: Détection de collisions dans CSMA/CD

Dès que les stations détectent une collision, les stations émettrices arrêtent la transmission de leurs messages, ce qui permet d'éviter d'occuper le canal jusqu'à la fin des transmissions en cours. Pour assurer que la collision est correctement interprétée

par les autres émetteurs, celles-ci renforcent la collision en transmettant une brève **séquence de brouillage** appelée ***jam*** avant d'arrêter leur émission. Dès qu'une station émettrice détecte une collision, elle transmet ce signal pour avertir les autres émetteurs. Sa durée est de 32 bits ce qui est suffisant pour qu'il soit détecté par tous les émetteurs. La collision est détectée parce que le signal transmit et le signal vu sur le média sont différents. Il est à noter qu'une station réceptrice ne peut pas détecter de collision puisqu'elle n'a pas de signal de référence pour comparer le signal vu sur le média. Elle détecte une violation de la méthode de codage qui peut être due à d'autres interférences. A cause de cela, elle traite les données reçues comme d'habitude mais détectera probablement l'erreur à cause du format incorrecte de la trame au d'une erreur de la somme de contrôle.

La retransmission de la trame s'effectue après un délai d'attente aléatoire (voir en-bas). Si, au bout de 16 essais, la trame n'est pas encore transmise, l'émetteur abandonne sa transmission et signale une erreur à la couche supérieure qui initie une reprise de la transmission.

L'algorithme complet et montré dans la Figure 15.

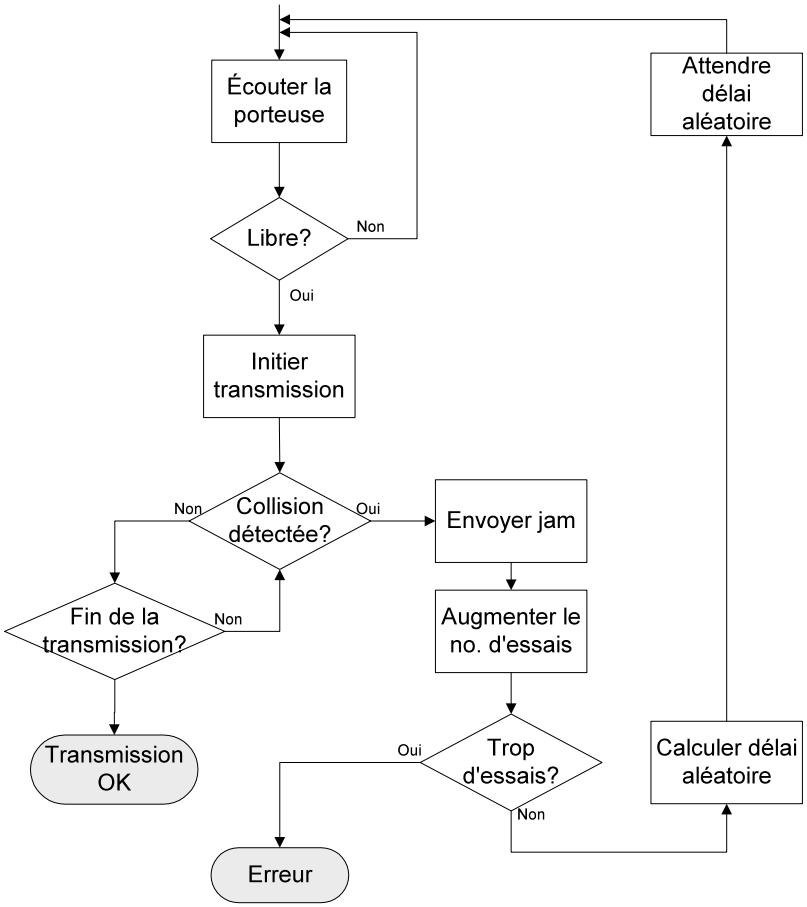


Figure 15: Diagramme de flux de CSMA/CD

Il est nécessaire de définir plusieurs paramètres pour pouvoir détecter correctement les collisions. Ces paramètres sont spécifiés dans la norme IEEE 802.3.

Temps aller-retour maximal : Le temps aller-retour maximal correspond au temps qui s'écoule entre les deux points les plus éloignés du réseau local, à partir de l'émission d'une trame jusqu'au retour d'un signal de collision. La norme définit un temps aller-retour maximal de **51,2 µs** ou de 512 temps d'émission d'un bit ou encore 512 temps élémentaires. Cette durée est aussi appelée la *fenêtre de collision*. La vitesse de propagation sur un câble coaxial étant approximativement 200 000 km/s, la portée maximale sur un même câble est de 5 km environ.

Taille minimale d'une trame : Un émetteur ne peut détecter une collision de trames que durant l'émission de la trame. La détection se base sur la comparaison du signal émis et du signal présent sur le canal. Un émetteur détecte une collision au plus tard après le temps aller-retour maximal du signal, d'où découle la taille minimale de 512 bits ou **64 bytes** d'une trame.

Longueur du signal jam. La séquence de bourrage est envoyée par les émetteurs de trames en collision afin de renforcer une collision. La durée d'une collision peut être très courte, par exemple lorsqu'une station commence à transmettre juste avant de détecter le signal de la transmission d'une autre station. Dans ce cas-là, elle cessera presque immédiatement la transmission. Pour donner aux circuits électroniques de la station distante le temps de correctement détecter la collision on utilise un signal jam pour renforcer la collision.

En plus de ces paramètres, la norme IEEE 802.3 définit encore un délai à respecter entre la les trames et la méthode de calcul du délai aléatoire à attendre après une collision.

Interframe gap. Après avoir transmis une trame, la station émettrice doit attendre un délai de 9,6 µs, (appelé interframe gap) avant de transmettre la prochaine trame. Ce temps est nécessaire pour les circuits électroniques des transceivers afin de préparer la prochaine réception.

Calcul du délai aléatoire. Après une transmission avortée par suite de collision, la station émettrice effectue jusqu'à 15 essais de retransmission. Afin d'éviter que plusieurs stations émettrices n'entrent à nouveau en collision en retransmettant toutes immédiatement après la collision, les instants de retransmission sont déterminés par un processus aléatoire de type TBEB (*Truncated Binary Exponential Backoff*). Avec cette méthode, l'instant de retransmission après la séquence de brouillage est un multiple rT de la fenêtre de collision T (51,2µs), où r est un entier aléatoire uniformément distribué, avec

$$0 \le r \le 2^m - 1$$
$$m = \min(n,10)$$

où n est le nombre de collisions déjà effectuées. Donc, après la première collision (n=1) une station doit attendre 0 ou 1 fois T avant de retransmettre (r=0 ou 1). Après la deuxième collision r=0, 1, 2, 3. Et ainsi de suite jusqu'à la 9ème collision consécutive. A partir de la 10ème collision consécutive, r=0, …, 1023.

On voit donc que le retard moyen de retransmission double approximativement après chaque essai infructueux. Il a été montré que cette augmentation exponentielle du

délai entre retransmissions est nécessaire pour garantir la stabilité du trafic dans le réseau. Sans cette méthode, les retransmissions pourraient fortement augmenter le trafic offert du réseau, ce qui provoque encore plus de collisions et de retransmissions et ainsi de suite jusqu'à l'effondrement du réseau.

4.2.2 Performances d'un réseau CSMA/CD

L'évaluation des performances d'un réseau utilisant CSMA/CD est complexe. Un travail important été réalisé sur l'analyse des performances de ce type de réseau. Des modèles analytiques ont été développés pour décrire le trafic écoulé en fonction du trafic offert. Cependant, ces modèles sont basés sur l'hypothèse d'un trafic dit poissonnien. Dès que les chercheurs ont commencé à examiner d'un peu plus près la réalité, ils se sont aperçus que le trafic était rarement poissonnien. Sans cette hypothèse, cependant, les modèles analytiques deviennent très complexes. Le modèle en-bas présent donc une approximation simple des performances.

Le trafic écoulé Y d'un réseau CSMA/CD peut être estimé comme

$$Y = \frac{1}{1 + \alpha \frac{B}{l} \mathrm{RTT}},$$

avec :

- α : constant empirique.
  Une valeur pessimiste est α=3,1, une valeur réaliste est α=2,5.
- B : Débit nominal de transmission du réseau (p.ex. B=10 Mb/s).
- l : taille moyenne des trames, y compris toutes les en-têtes.
- RTT : Temps aller-retour maximal du réseau (*Round-Trip-Time*).
  Selon la norme IEEE 802.3, RTT ≤ 51,2 μs.

La Figure 16 montre le trafic écoulé en fonction de la taille l des trames. Les paramètres sont α = 2,5, B = 10 Mb/s. La valeur du délai aller-retour est RTT = 51,2 μs, donc modélisant un très grand réseau.

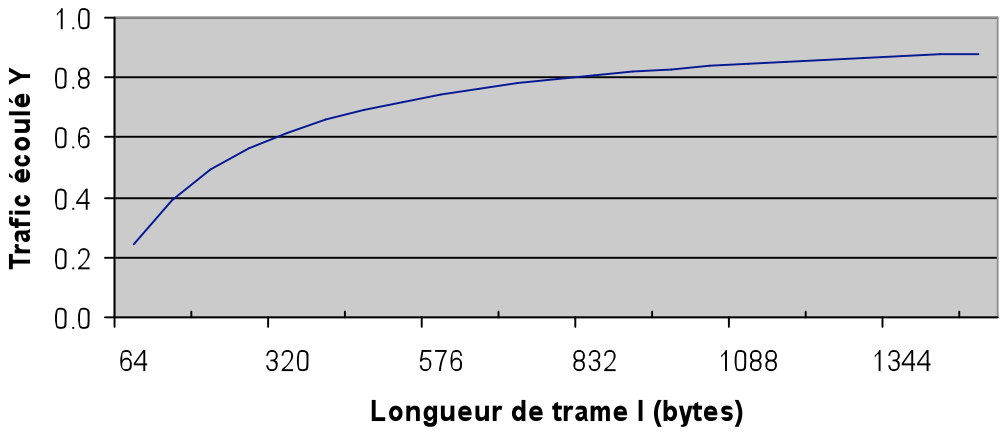


Figure 16: Trafic écoulé d'un réseau CSMA/CD en fonction de la longueur de trame

On peut voir que le trafic écoulé est très petit pour une taille de trame minimale de 64 bytes. Le trafic écoulé croît avec la taille de trame et avoisine 90 % pour de grandes trames. Pour une taille moyenne réaliste d'environ 600 bytes, on obtient un trafic écoulé d'environ 75 %.

Comme indique précédemment, ce modèle est basé sur l'hypothèse peu réaliste d'un trafic poissonnien. Des mesures ont montré que le trafic réel dans les réseaux locaux et beaucoup plus agressif que le trafic poissonnien. Les valeurs obtenues à l'aide de notre modèle doivent donc être interprétées avec un brin de bon sens et indiquent plutôt les performances dans le meilleur des cas.

4.2.3 Le format de trame Ethernet

Les trames sont construites par la sous-couche MAC à l'exception du préambule qui lui est généré par des sous couches inférieures.

La Figure 17 montre qu'il existe deux types de trames MAC:

- la trame selon le standard IEEE 802.3 et
- la trame MAC Ethernet-II.

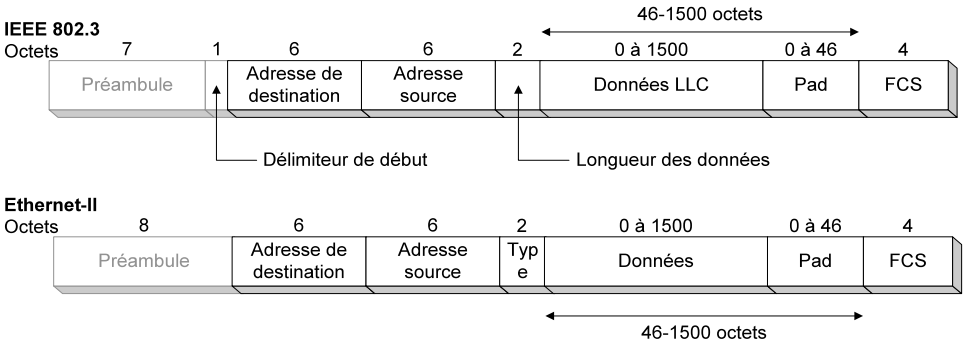


Figure 17: Les formats des trames MAC IEEE 802.3 et Ethernet-II

Ces deux trames sont légèrement différentes:

- La première différence concerne le nombre d'octets définissant le préambule. La trame IEEE 802.3 commence avec un préambule de 7 octets consistant en octets 10101010. Le délimiteur de début *(Start of Frame Delimiter*, SOF*)* suit le préambule et contient la valeur 10101011.
  Le préambule de la trame Ethernet-II comprend 8 octets dont les premiers 7 avec la valeur 10101010 et le dernier avec la valeur 10101011.
  Le préambule et le SOF de la trame IEEE 802.3 correspondent donc exactement au préambule de la trame Ethernet-II.

- La deuxième différence concerne les deux bytes qui suivent l'adresse source. Dans une trame IEEE 802.3 ce champ indique la longueur du champ des données LLC. Dans une trame Ethernet-II ce champ définit **type du protocole** encapsulé dans le champ des données. La Table 1 indique les principaux types actuellement définis. D'après ce tableau on voit que les valeurs attribuées aux différents types sont toujours supérieures à 05DC hex (1500 décimal), donc la longueur maximale du champ des données LLC. Si donc la valeur de ces deux bytes est supérieure à 1500 il faut interpréter la trame comme une trame MAC Ethernet-II et non pas MAC IEEE 802.3.
  Dans le cadre d'une trame MAC IEEE 802.3 on ne peut connaître le type de protocole encapsulé dans le champ des données que si l'on analyse les premiers bytes de ce champ p. ex. les bytes DSAP et SSAP de l'en-tête LLC (voir Section 3.1).

Table 1: Type de protocoles encapsulés dans une trame Ethernet

Protocole	Code (hexadécimal)	Protocole	Code (hexadécimal)
IP	0800	DEC LAT	6004
X.75 Internet	0801	DEC Diagnostic Protocol	6005
X.25 Level 3	0805	DEC LANBridge	8038
ARP	0806	DEC Ethernet Encryption	803D
Banyan Systems	0BAD	AppleTalk	809B
BBN Simnet	5208	IBM SNA Service on Ethernet	80D5
DEC MOP Dump/Load	6001	AppleTalk ARP	80F3
DEC MOP Remote Console	6002	NetWare IPX/SPX	8137
DEC DECNET Phase IV Route	6003	SNMP	814C

Actuellement pratiquement toutes les cartes réseau (NIC *Network Interfaces Card*) sont capables de décoder ces différents types de trame MAC. Cependant, pour la transmission de paquets TCP/IP, la plupart des ordinateurs utilisent le format Ethernet-II.

Le champ préambule est nécessaire pour permettre aux horloges des récepteurs de se synchroniser avec l'horloge de l'émetteur. Le dernier octet dans le préambule d'une trame Ethernet ou le champ **SOF** dans une trame IEEE 802.3 signalisent le début de la trame.

Le champ des données LLC, issu de la couche LLC, n'est pas modifié par la couche MAC. Il contient les données utiles (données faisant partie du message initial) et

des informations rajoutées par les couches supérieures. Il peut contenir la totalité du message initial ou seulement une fraction de celui-ci. La taille de ce champ varie de 0 à 1518 octets.

Pad. Une taille de trame minimum de 64 octets (sans compter le préambule et le SOF) est imposée par le protocole 802.3. Il existe un champ de remplissage (***padding***) qui est remplie avec jusqu'à 46 octets pour arriver à la taille minimum imposée si la longueur des données LLC est inférieure à 46 octets.

FCS. La trame se termine par séquence de contrôle d'erreurs (*Frame Control Sequence*) de 32 bits qui est calculé avec un code polynomial CRC (*Cyclic Redundancy Check*). La vérification d'erreurs porte sur tous les champs, sauf le préambule et le délimiteur de début. La trame ne comporte pas de délimiteur de fin, car le champ de longueur permet de repérer sans ambiguïté la fin de la trame.

Contrairement aux autres réseaux, dans les réseaux IEEE 802 il n'existe qu'un seul type de trame, car le protocole d'accès de type Ethernet ne nécessite pas de trame spécialisée pour gérer l'accès au réseau, la reprise ou l'initialisation. Toutes ces fonctions se règlent au niveau local, sans la mise en œuvre d'un protocole entre pairs.

VLAN tagging

Une extension du format des trames MAC dans IEEE 802.3 a été normalisée afin de permettre la définition de réseaux locaux virtuels (VLAN, voir Section 0) et de classes de trafic avec une qualité de service différente. Le format de trame selon cette norme IEEE 802.1Q est montré dans la Figure 18.

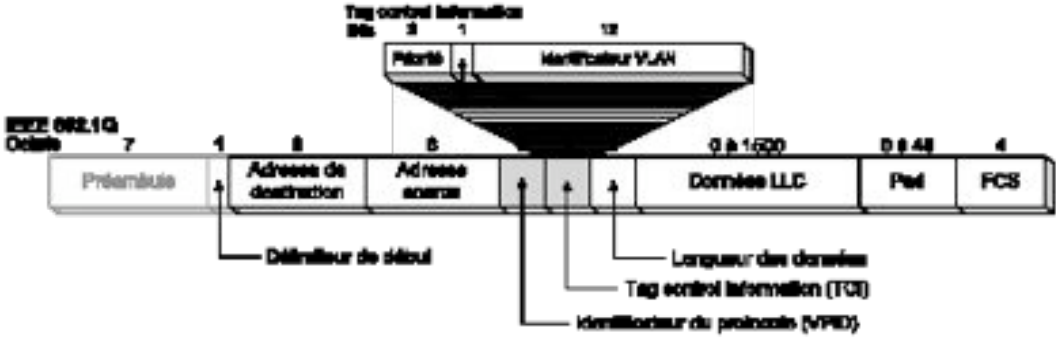


Figure 18: Format de trame selon IEEE 802.1Q (VLAN tagging)

Deux champs supplémentaires sont introduits dans ce format.

Identificateur du protocole. Ce champ VPID (VLAN protocole identifier) à la valeur 8100 hex pour indiquer qu'il s'agit d'une trame utilisant le format IEEE 802.1Q. Il permet donc de distinguer ces trames des trames IEEE 802.3 qui ont le champ de la longueur à cette place avec une valeur d'au maximum 08DC hex (1500 décimal).

Tag control information. Le champ TCI contient lui-même trois champs :

- Un champ de priorité de 3 bits permettant jusqu'à huit niveaux de priorité.

- Un champ d'un bit, le bit CFI (*Canonical Format Indicator*), qui n'est pas utilisé dans les réseaux IEEE 802.3 et doit être mis à 0 dans ce cas. On lui attribue la valeur 1 pour des encapsulations de trames Token Ring.
- Un champ d'identificateur VLAN (VID, VLAN identifier) de 12 bits, qui indique le VLAN dont font partie la source et le destinataire de la trame.

Ce format de trame ne peut être utilisé que si tous les nœuds du réseau local (stations, commutateurs, …) implémentent la norme IEEE 802.1Q.

Encapsulation des PDUs dans les trames Ethernet

Plusieurs méthodes d'encapsulation de PDUs des couches supérieures dans les trames Ethernet sont utilisées.

Pour la transmission de datagrammes IP sur un réseau Ethernet, presque tous les ordinateurs utilise aujourd'hui une encapsulation directe du datagramme IP dans une trame Ethernet-II. Dans ce cas, la valeur du champ 'Type' de la trame Ethernet-II contient la valeur 0800 hex pour indiquer qu'un datagramme IP est transporté. Cette encapsulation est montrée dans la Figure 19.

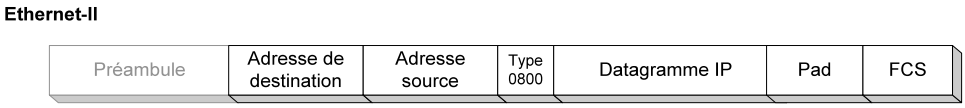


Figure 19: Encapsulation d'un datagramme IP dans une trame Ethernet-II

L'encapsulation de datagrammes IP dans des trames IEEE 802.3 est rare est doit obligatoirement utiliser l'encapsulation SNAP.

Encapsulation SNAP. L'encapsulation *Ethernet Subnetwork Access Protocol* est standardisée dans IEEE 802.3 et permet de transporter différents types de protocoles **non-IEEE** des couches supérieures, comme p. ex. AppleTalk ou IP, sur un réseau de type IEEE 802.3. Le format de trame IEEE 802.3 reste inchangé. Cependant, dans la PDU LLC, un code AA hexadécimal pour SSAP et DSAP et de 03 hex pour le champs 'Contrôle' indiquent que l'encapsulation SNAP est utilisée. L'en-tête SNAP suit l'en-tête LLC et contient les deux champs :

- **OUI** (*Organizational Unit Identifier*) : Champs de 3 octets identifiant l'organisation ou l'autorité qui a structuré les données dans les champs qui suivent.
- **Type** : Champs de deux octets qui spécifie le type de protocole encapsulé. Pour un datagramme IP, ce champ contient la valeur 0800 hex.

La trame résultant est montrée sur la Figure 20. Une description complète de SNAP se trouve dans la RFC 1042.

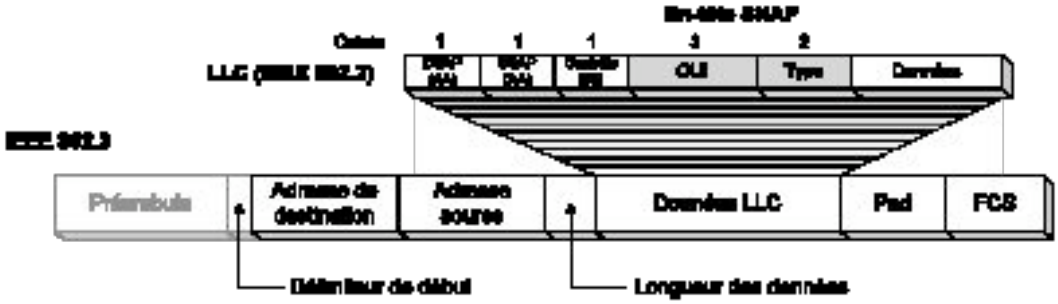


Figure 20: Encapsulation SNAP dans une trame IEEE 802.3

L'encapsulation d'un protocole IEEE d'une couche supérieure dans une trame IEEE 802.3 utilise le format LLC. La PDU du protocole supérieure est encapsulé dans une PDU LLC et ensuite dans la trame IEEE 802.3. Dans ce cas-là, les champs SSAP et DSAP de la PDU LLC indiquent le protocole encapsulé.

L'encapsulation directe (sans LLC) d'une PDU d'une couche supérieure dans une trame IEEE 802.3 est aussi possible. Cependant, comme aucun champ de la trame résultant indique le protocole encapsulé, un seul protocole peut utiliser cette méthode sans causer de confusion. Ce protocole est Novell IPX.

4.2.4 Adresses MAC

Une adresse MAC est l'adresse physique d'une carte réseau. Elle est utilisée dans les trames des réseaux locaux pour indiquer la source et le destinataire. Selon les normes les adresses peuvent être codées sur 16 ou 48 bits. Dans la pratique uniquement les adresses à 48 bits ont été implémentées par les constructeurs.

L'adresse MAC d'une carte réseau est configurée dans sa mémoire ROM et ne peut pas être changée. Les adresses MAC sont uniques: l'IEEE attribue à chaque constructeur un numéro spécifique de 6 chiffres hexadécimaux compris dans les trois premiers octets. Le constructeur gère lui-même les autres bits disponibles de l'adresse c'est à dire les trois octets restant. Il ne faut s'attendre à aucune logique dans la numérotation quand on considère un réseau particulier. Une liste non exhaustive des adresses des vendeurs se retrouve dans le RFC 1340.

Attention Une source de confusion est l'ordre de transmission des bits dans les réseaux LAN. Dans un réseau Ethernet, le bit le plus significatif est transmis *en dernier*. Par contre, dans un réseau Token Ring, le bit le plus significatif est transmis *en premier*.

Le bit le moins significatif du premier octet d'une adresse MAC (voir Figure 21 pour une adresse Ethernet, où ce bit est le premier bit transmis) spécifie s'il s'agit d'une adresse individuelle (adresse aussi appelée *unicast)* ou de groupe. Une valeur de ce bit de 0 indique une adresse individuelle, une valeur de 1 une adresse de groupe. Les adresses de groupe ont donc un **premier octet** qui est **impair** (p.ex. 09-00-2B-00-00-90).

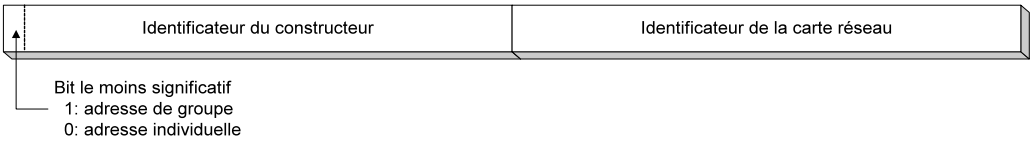


Figure 21: Format d'une adresse MAC

En résumé les adresses MAC sont universelles et désignent de manière unique une station dans le monde entier. Cette propriété est très importante et sera utilisée pour la configuration automatique des stations.

Adresses de groupe

L'adresse de groupe la plus utilisée est appelée **broadcast** et a la forme **FF-FF-FF-FF-FF-FF** selon la notation hexadécimale.
L'adresse de *broadcast* est utilisée pour adresser toutes les stations d'un réseau et correspond à une adresse de diffusion générale.

Le broadcast est utilisé, par exemple, quand une station ne connaît pas l'adresse MAC du destinataire mais par exemple uniquement son adresse IP. Elle envoie alors le message à l'ensemble des stations du réseau. La station qui connaît l'adresse du destinataire (généralement le destinataire lui-même) répond en envoyant son adresse MAC.

L'inconvénient majeur du broadcast, provient du filtrage des messages par les couches hautes (c'est-à-dire chaque message de broadcast doit être analysé par les couches >2), ce qui se traduit par une perte de performance de l'ensemble des stations du réseau.

Un cas particulier de l'adresse de groupe est l'adresse **multi-cast** (à destination d'un groupe de stations). L'adresse de multi-cast est utilisée uniquement en tant qu'adresse de destination pour adresser un groupe de stations disposant par exemple d'une même application ou fonction réseau. Par exemple dans le cadre de l'utilisation de l'algorithme du « *spanning tree* » tous les ponts (bridges) dans un réseau sont amenés à échanger des messages au moyen d'une adresse multi-cast réservée à cet effet.

Pour le multi-cast, les stations qui veulent accéder à un service ou groupe doivent explicitement s'abonner. Elles donnent explicitement à la couche MAC l'adresse du groupe. Quand MAC reconnaît un paquet portant une adresse de groupe préalablement enregistrée, il transmet ce paquet aux couches supérieures. Le filtrage se fait directement au niveau de la carte (contrôleur) par le protocole MAC et ne pénalise pas les stations.

4.3 Types de réseaux Ethernet

La norme IEEE 802.3 ne décrit pas un seul type de réseau local mais toute une famille de technologies, basées sur la méthode CSMA/CD et le format de trame décrit dans la section précédente. Historiquement, les premiers réseaux Ethernet travaillaient avec un débit de 10 Mb/s sur un câble coaxial comme média partagé. Avec l'arrivée de nouvelles applications téléinformatiques, l'IEEE s'est vu obligé de définir de nouvelles technologies plus performantes afin de satisfaire la demande croissante de débit de transmission. Au lieu d'introduire une technologie complètement nouvelle,

l'IEEE a choisi de « gonfler » la norme 802.3, surtout en vue d'une compatibilité ascendante avec les produits 802.3 existant sur le marché.

Les différents modes de fonctionnent sur un média sont décrits dans les différents chapitres de la norme IEEE 802.3. Chaque mode porte un nom composé de trois éléments :

1. Débit de la transmission en Mb/s
2. Technique de codages des signaux :
    a. Bande de base : Base
    b. Large bande (modulation) : Broad
3. Identificateur du média ou longueur maximale d'un segment, en centaine de mètres.

La Table 2 donne les principaux média actuellement utilisés.

Table 2: Les différents types d'Ethernet

Type	Débit	Codage	Longueur max. d'un segment	Média	Topologie
10Base-5	10 Mb/s	Bande de base	500 m	Câble coax. épais	Bus
10Base-2	10 Mb/s	Bande de base	185 m	Câble coax. fin	Bus
10Base-T	10 Mb/s	Bande de base	100 m	UTP cat. 3, 2 paires	Étoile
100Base-TX	100 Mb/s	Bande de base	100 m	UTP cat. 5, 2 paires	Étoile
100Base-FX	100 Mb/s	Bande de base	2000 m	2 fibres multimodes	Étoile
1000Base-T	1 Gb/s	Bande de base	100 m	UTP cat. 5, 4 paires	Étoile
1000Base-X (plusieurs normes)	1 Gb/s	Bande de base	275-5000 m	2 fibres optiques	Étoile

Les différents types d'Ethernet se distinguent surtout par le support physique utilisé et le débit de transmission. Cependant, le débit de transmission influence aussi d'autres caractéristiques d'un réseau comme la taille maximale du réseau ou la taille minimale d'une trame.

4.3.1 Ethernet 10 Mb/s

4.3.1.1 10Base-5

Historiquement, le mode 10Base-5 a été le premier mode utilisé. Le média physique est un câble coaxial d'une épaisseur de 1,02 cm et une impédance de 50 ohms. À cause de l'épaisseur du câble, ce type d'Ethernet est aussi appelé *Thicknet*. Ce câble ressemble à un tuyau d'arrosage de couleur jaune avec des repères tous les 2,5 m pour

désigner les emplacements des prises de raccordement. Le raccordement mécanique au câble est réalisé au moyen d'une prise particulière appelée *prise vampire*. Au niveau de chaque prise, un petit trou percé dans le câble coaxial permet à de fines pointes d'entrer en contact avec l'âme centrale du câble et avec la tresse métallique périphérique (Figure 22).

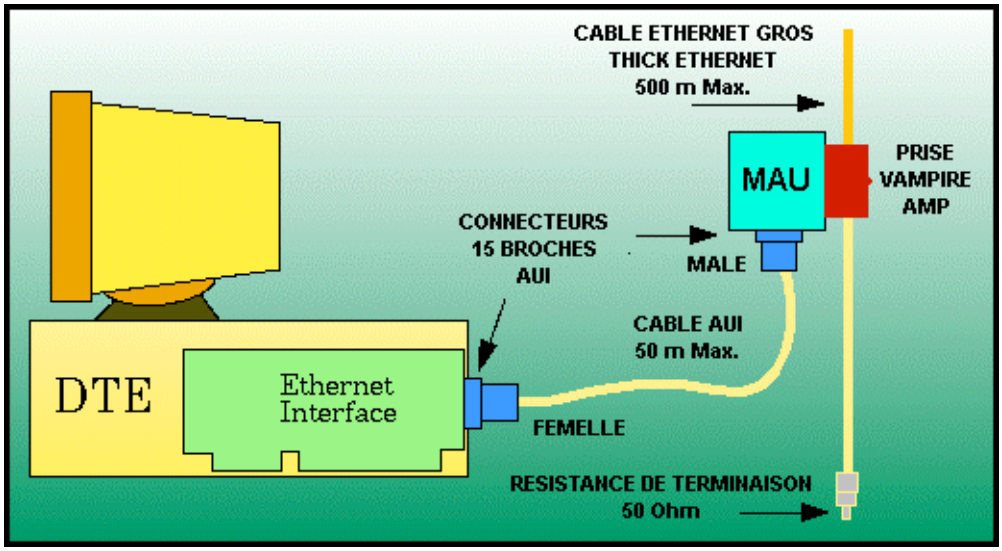


Figure 22: Connexion d'une station à un segment Thicknet

Transceiver

Un circuit transmetteur-récepteur appelé transceiver ou MAU (*Media Adapter Unit*) est raccordé au câble. Le transceiver contient les composants électriques de transmission et de réception, de même que ceux qui sont spécifique à la détection de collisions. Le transceiver est relié à la carte réseau par un cordon de raccordement spécial, le **câble AUI** (*Attachment Unit Interface*) qui comprend cinq paires torsadées blindées. Sa longueur ne doit pas dépasser **50 m**. Certains transceivers permettent de raccorder jusqu'à huit stations proches les unes des autres, dans un souci de réduire le nombre de transceivers nécessaires.

Segment

Le câble coaxial qui sert de support partagé auquel les stations sont connectées est appelé **segment**. Sa longueur ne doit pas dépasser 500 m à cause de l'affaiblissement des signaux. Le segment doit être terminé à chacune de ses extrémités par une résistance de 50 ohms pour éliminer des réflexions. Une des extrémités doit être mise à terre. La norme permet de raccorder jusqu'à **100 stations à un segment** 10Base-5.

La Table 3 résume les caractéristiques d'un segment 10Base-5.

Table 3: Caractéristiques d'un segment 10Base-5

Paramètre	
Media physique	Câble coaxial

Diamètre du câble	1 cm (0,4 pouces)
Impédance caractéristique	50 ohms
Coefficient de vélocité	0,77
Atténuation	8,5 dB sur 500 m à 10 MHz
Débit de transmission	10 Mb/s
Longueur maximale d'un segment	500 m
Nombre maximal de stations par segment	100

La rigidité du câble, son diamètre et son coût font que 10Base-5 n'est pratiquement plus utilisé aujourd'hui. Son emploi est réservé aux sites nécessitant un segment long ou une bonne protection contre les interférences électromagnétiques.

Répéteurs

La puissance des signaux délivrés par les transceivers ne permet pas une transmission au-delà d'une longueur de câble de 500 m. Pour couvrir des distances plus longues ou pour connecter plus de 100 stations à un réseau 10Base-5, plusieurs segments doivent être utilisés. Les segments sont interconnectés par des *répéteurs* (Figure 23).

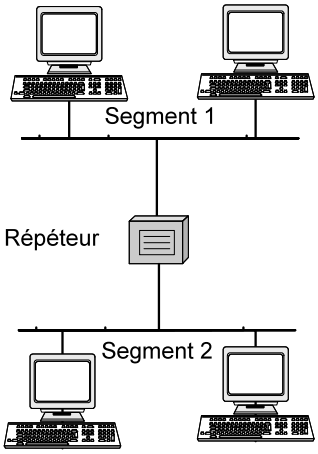
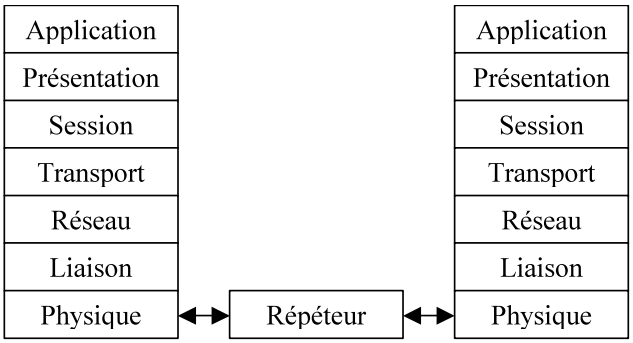


Figure 23: Segments interconnectés par un répéteur

a) Répéteur



b) Répéteur dans le modèle OSI

Figure 24: Répéteur

Un répéteur (Figure 24) régénère le signal afin de permettre la transmission sur une distance plus élevée. Il travaille au niveau de la *couche physique* du modèle OSI donc au niveau de la transmission des bits individuels. Il ne décode pas les trames qu'il reçoit, il se contente uniquement de les transmettre bit par bit sur d'autres segments.

Le répéteur, comme tout équipement Ethernet capable d'émettre des trames, doit pouvoir gérer les collisions que lui-même génère ou celles générées par les autres équipements présents sur le câble. Il faut distinguer en cas d'apparitions d'une collision sur un des segments deux comportements différents du répéteur:

- Collision provoquée par un des équipements rattachés sur des segments du répéteur.
- Collision provoquée par le répéteur lui-même.

Collision provoquée par un des équipements rattachés sur des segments du répéteur. Lorsqu'une collision apparaît sur un segment, il reste sur ce segment un fragment de trame qui se propage jusqu'aux extrémités du câble. Lorsque le répéteur perçoit cette collision sur un de ses ports, il va essayer de propager cette information sur tous les autres segments auquel il est rattaché. Afin que le fragment (collision) soit assez long pour être détecté par tous les équipements connectés sur les différents segments rattachés à ses ports, le répéteur effectue si nécessaire une extension du fragment à une longueur minimale de 96 bits en ajoutant de signal jam.

Collision provoquée par le répéteur lui-même. Le répéteur peut naturellement être source de collisions lorsqu'il reçoit une trame d'un côté et en vertu de sa fonction de répéteur, il la propage su le ou les autres segments. Le répéteur dans ce cas il se comporte comme n'importe quelle autre station c'est-à-dire:

- il arrête de transmettre sa trame et
- émet le signal jam sur tous les segments auxquels il est raccordé et
- ensuite, à la différence d'une station, le répéteur ne cherche pas à ré-émettre sa trame. C'est la station initiale d'émission qui après détection du jam, lance le processus de répétition.

Comme un répéteur propage les collisions, tous les segments interconnectés par des répéteurs font partie du même **domaine de collision**. Les stations ne détectent pas la présence de répéteurs et voient le réseau comme comprenant un seul segment.

Interconnexion de segments 10Base-5

Pour assurer qu'un réseau de segments interconnectés fonctionne correctement, le temps de propagation aller-retour d'un signal à travers le réseau ne doit pas dépasser le temps maximal de 51,2 μs. À cause de cela, la norme IEEE 802.3 limite le nombre maximum de répéteurs *entre deux stations* à **4 répéteurs**. La chemin maximal entre deux stations comprend donc 5 segments interconnectés. La norme spécifie également qu'au maximum 3 de ces 5 segments peuvent être des **segments principaux**, c'est-à-dire avec des stations connectées. Les segments sans stations sont appelés **câbles intersegments** (IRL, *Inter-Repeater Link*) et servent à connecter des segments principaux. Ces segments de liaison sont des câbles **en fibre optique** ou en **paires**

torsadées. La longueur totale de tous les segments de liaison ne doit pas dépasser 1000 m.

La limitation du nombre de répéteurs et des segments porte aussi le nom de la **règle 5-4-3-2-1** :

- 5 segments interconnectés par
- 4 répéteurs,
- 3 segments principaux
- 2 segments de liaison
- 1 domaine de collision.

La Figure 25 montre un chemin maximal entre deux stations. L'étendue maximale peut être calculée comme suivant :

3 segments principaux (500 m chacun)	1500 m
2 segments de liaison	1000 m
6 câbles AUI pour la connexion aux segments principaux (50 m chacun)	300 m
Etendue maximale	**2800 m**

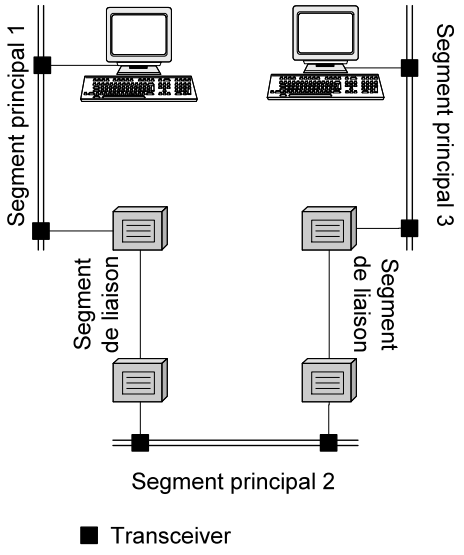


Figure 25: Chemin maximal entre deux stations dans un réseau 10Base-5

La résume les paramètres et règles d'un réseau 10Base-5.

Table 4: Paramètres et règles d'un réseau 10Base-5

Paramètre	
Longueur maximale d'un segment	500 m
Longueur maximale d'un câble transceiver	50 m
Nombre maximal de segments principaux	3

Nombre maximal de segments de liaison	2
Longueur maximale de segments de liaison	1000 m
Nombre maximal de stations par segment	100
Nombre total de stations	1024
Distance minimale entre deux stations	2,5 m

4.3.1.2 10Base-2

Les réseaux 10Base-5 ont l'inconvénient majeur de la rigidité et le coût du câble. Un autre câble coaxial moins encombrant et plus souple à été normalisé sous l'appellation 10Base-2. Ce câble, connu aussi sous les noms *Thinnet* ou *Cheapnet*, a les caractéristiques montrées dans la Table 5.

Table 5: Caractéristiques d'un segment 10Base-2

Paramètre	
Media physique	Câble coaxial
Diamètre du câble	0,48 cm
Impédance caractéristique	50 ohms
Coefficient de vélocité	0,65
Débit de transmission	10 Mb/s
Longueur maximale d'un segment	185 m
Nombre maximal de stations par segment	30

La Figure 26 montre quelques éléments d'un réseau Ethernet en câble coaxial fin.

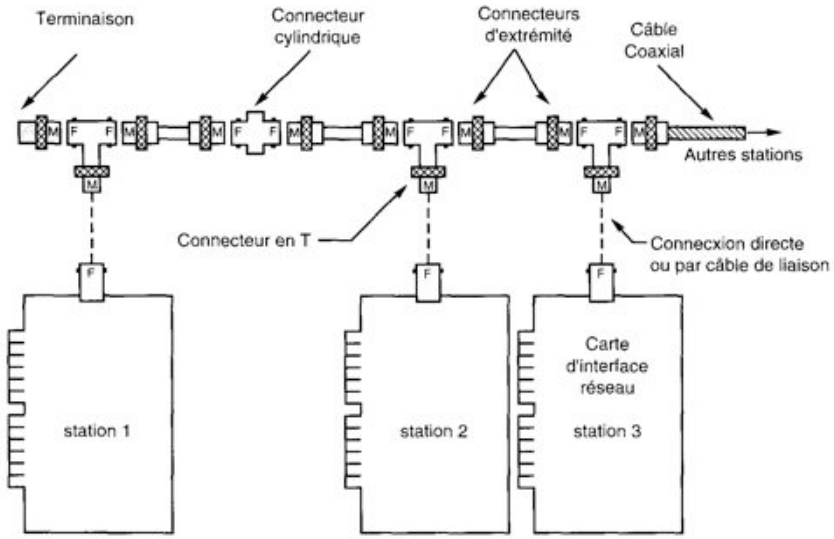


Figure 26: Eléments d'un réseau 10Base-2

Les fonctions des transceivers d'un réseau en 10Base-2 sont effectuées par la carte réseau. Il n'est donc pas nécessaire d'installer de transceiver sur le réseau. Des connecteurs en T relient les cartes au câble. Les deux extrémités opposées d'un T permettent de connecter deux segments de câble fin pour continuer le bus.

La longueur d'un câble fin ne peut excéder 185 mètres, à cause de l'atténuation des signaux. Le câble fin est de type RG-58. Son diamètre est d'environ 0,5 centimètres,

et son impédance de 50 ohms. Ce câble est disponible en longueurs fixes, et les extrémités contiennent les connecteurs BNC. Vous pouvez fabriquer des câbles de longueur quelconque et sertir les connecteurs BNC au moyen d'une pince spéciale.

Vous pouvez aussi utiliser des prolongateurs BNC pour relier deux segments de câble. Un segment doit être terminé aux deux extrémités par une résistance de 50 ohms. Une seule résistance de terminaison doit être mise à la terre.

Les règles d'interconnexion de segments sont les mêmes que pour un réseau 10Base-5. La règle 5-4-3-2-1 est donc valable aussi pour les réseaux 10Base-2.

La Table 6 recense les différentes règles à respecter dans un réseau Ethernet en câble coaxial fin.

Table 6: Paramètres et règles d'un réseau 10Base-2

Paramètre	
Longueur maximale d'un segment	185 m
Nombre maximal de segments principaux	3
Nombre maximal de segments de liaison	2
Longueur maximale de segments de liaison	1000 m
Nombre maximal de stations par segment	30
Nombre total de stations	1024
Distance minimale entre deux stations	0,5 m

4.3.1.3 10Base-T

Le problème de la détection de rupture de câble coaxial ou d'autres défaillances ainsi que la baisse des prix des éléments actifs de réseau ont conduit dans les années 90 les systèmes de câblage vers des *configurations en étoile*. Sur ce nouveau schéma de câblage on distingue un système central, le **hub**, vers lequel convergent les câbles des stations. Les câbles de raccordement des stations sont de simples câbles téléphoniques à paires torsadées. Ce schéma de câblage est appelé **10Base-T**. L'emploi de câbles existants mais non utilisés dans les bâtiments a rendu ce schéma très économique. La Figure 27 montre une configuration 10Base-T simple.

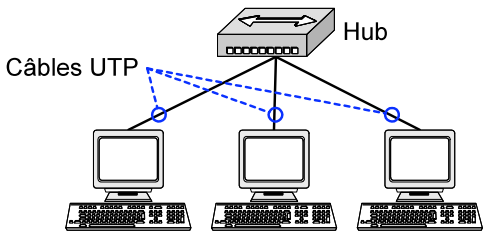


Figure 27: Exemple d'une configuration 10Base-T

Câbles 10Base-T

Contrairement aux réseaux 10Base-5 et 10Base-2 la norme 10Base-T ne se base pas sur un câble très précisément défini. Elle donne plutôt des niveaux de performances en transmission de signaux.

Les caractéristiques des câbles 10Base-T sont données dans la Table 7.

Table 7: Caractéristiques de la norme 10Base-T

Paramètre	
Média physique	Câble de paires torsadées
Impédance caractéristique	100 ohms
Coefficient de vélocité	0,585
Débit de transmission	10 Mb/s
Longueur maximale d'un segment	100 m
Nombre de stations par segment	2

Sur un segment il n'y a que deux équipements connectés chacun à une extrémité. La carte réseau effectue les fonctions du transceiver. Le raccordement est prévu avec un connecteur RJ-45 de 8 broches (Figure 28).

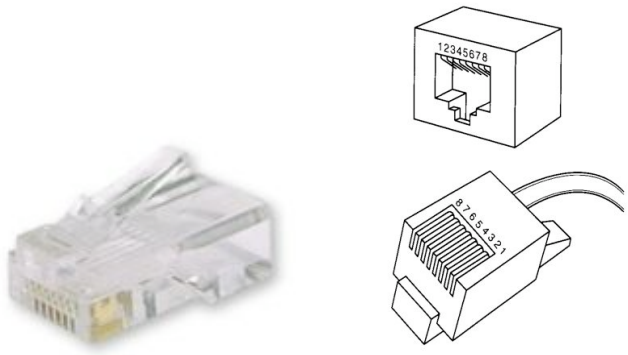


Figure 28: Connecteur RJ-45

Seulement 4 broches du connecteur sont utilisées en 10Base-T:

Broche	Signal
1	Transmission +
2	Transmission –
3	Réception +
4	Non utilisé en 10Base-T
5	Non utilisé en 10Base-T
6	Réception –
7	Non utilisé en 10Base-T
8	Non utilisé en 10Base-T

Câbles à paires torsadées

Le plus ancien support de transmission et le plus largement utilisé est le câble électrique à paires torsadées. Une paire torsadée est composée de deux conducteurs en cuivre, isolés l'un de l'autre, et enroulés de façon hélicoïdale. Pourquoi ces torsades ? Pour des raisons de performance de transmission. En effet ces torsades:

1. Diminuent la sensibilité aux perturbations électromagnétiques. Quand un signal parasite perturbe un conducteur, il perturbe à peu près de la même manière le deuxième conducteur.

2. Diminuent la perturbation du câble en augmentant l'inductance du câble.

3. Et enfin diminuent la paradiaphonie entre paires.

Un câble à paires torsadées comprends plusieurs paires torsadées, avec écran ou non, entourées par une tresse métallique de blindage si nécessaire et par une gaine extérieure dont la nature dépend du milieu environnant (humidité, rongeurs, risque d'écrasement, etc.).

La bande passante d'un câble électrique à paires torsadées dépend essentiellement de la section et de la qualité des conducteurs et isolants, ainsi que de la longueur utile. Le diamètre maximal du conducteur isolé est en principe limité par les possibilités du connecteur, par le prix du cuivre et par le volume qu'il occupe. Le diamètre du conducteur varie le plus souvent entre 0.1 et 0.8 mm, ce que signifie un diamètre total compris entre 0.3 et 1.5 mm pour le conducteur isolé.

Dans le cadre de l'utilisation des paires torsadées dans les connexions dans les réseaux locaux on distingue deux types de câbles torsadés:

- Les câbles de type **UTP** (*Unshielded Twisted Pair*): en paires torsadées avec une impédance caractéristique de 100 ohms et une atténuation de 24 dB/km. Les paires ne sont pas écrantées et donc le câble est plus flexible qu'un câble STP. Les câbles UTP présentent des caractéristiques de transmissions telles qu'ils sont prévus pour transmettre des signaux jusqu'à 100MHz

- Les câbles **STP** (*Shielded Twisted Pair*): Ces câbles ont été développés par IBM pour les réseaux Token Ring. Ces câbles en paires torsadées avec une impédance caractéristique de 150 ohms et une atténuation de 10dB/km. Les paires sont écrantées. Les câbles STP présentent des caractéristiques de transmissions telles qu'ils sont prévus pour transmettre des signaux jusqu'à 300MHz.

Les câbles UTP sont eux même groupés en catégories en fonction de leur qualité donc du débit admissible:

- Catégorie 1: câble pour voix et transmission de donnée à faible vitesse (max 56 Kb/s).

- Catégorie 2: câble pour transmissions jusqu'à 1 MHz.

- Catégorie 3: câble pour transmission jusqu'à 16 MHz. Ces câbles sont essentiellement prévus pour un usage à 10 Mb/ s sur 100 m.

- Catégorie 4: câble pour transmission jusqu'à 20 MHz. Ces câbles sont essentiellement prévus pour un usage à 16 Mb/s sur 100 m (utilisés p. ex dans les réseaux Token Ring)

- Catégorie 5: câble pour transmission jusqu'à 100 MHz. Ces câbles sont essentiellement prévus pour les hauts débits et utilisés p. ex: dans le cadre du FastEthernet, du FDDI sur cuivre CDDI ou des liaisons ATM jusqu'à 155 Mb/s.

- Catégorie 5e: câble pour transmission jusqu'à 100 MHz. Ce type de câble est souvent utilisé dans les installations actuelles. Il permet la transmission à 1 Gb/s avec Gigabit-Ethernet.

- Catégorie 6: câble pour transmission jusqu'à 200 MHz. Comme la catégorie 5e, cette catégorie est utilisée pour Gigabit-Ethernet et offre un très bon rapport signal-sur-bruit.

Les réseaux 10Base-T utilisent des câbles UTP de catégorie 3 ou plus haute.

Croisement des paires du câble

Pour qu'une transmission entre deux éléments du réseau 10Base-T soit possible, la paire d'émission (broches 1 et 2) de la source doit être connectée à la paire de réception du destinataire. Cependant, comme les deux côtés utilisent les mêmes connecteurs, il doit y avoir un croisement des paires. Dans les hubs, cette fonction de croisement est normalement effectuée au niveau des ports par un croisement interne. Un port avec un croisement interne doit être marqué du symbole X. Une station est connectée à un tel port à l'aide d'un câble appelé 'droit', donc sans croisement des paires.

Si un hub est connecté à un autre hub, un câble 'croisé' doit être utilisé où la paire de réception à un bout (broches 1 et 2), doit être connectée sur les broches de la paire de sortie de l'autre bout (broches 3 et 6). Le même câble croisé est utilisé pour connecter directement deux stations l'une à l'autre.

La Figure 29 montre les deux possibilités du croisement.

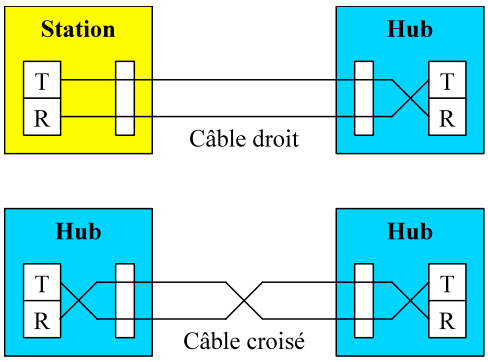


Figure 29: Croisement des paires du câble 10Base-T

Hubs

L’introduction du 10Base-T a révolutionné le câblage des réseaux locaux en raison de la grande souplesse et simplicité qui désormais permet d’adapter très facilement la configuration d’un réseau aux évolutions d’une entreprise où la mobilité des places de travail est de plus en plus nécessaire.

Le principe de fonctionnement d’un réseau 10Base-T reste cependant basé sur une topologie en bus. Un des deux équipements connectés sur le segment en paires torsadées doit donc restituer à partir de la topologie physique d’étoile une topologie logique de bus. C’est le rôle du hub.

Figure 30: Un hub à 9 ports

Un hub peut-être considéré comme un **répéteur multi-port**. Il travaille donc au niveau de la couche physique. Conceptuellement un hub consiste en plusieurs répéteurs (un par port) qui sont interconnectés par un bus intern. Les fonctions d’un hub sont les mêmes que celles d’un répéteur : il reçoit, contrôle et régénère les signaux de chaque station raccordée sur chacun de ses ports. Optionnellement, un hub peut effectuer les fonctions suivantes :

- Test de l’intégrité du lien
- Auto-partition du réseau pour déconnecter des segments défectueux

Test de l’intégrité du lien. Un hub test de façon active le fonctionnement de chaque transceiver des stations raccordées à l’un de ses ports: la fonction *link detection* permet, en l’absence de trames, de valider en permanence la qualité de liaison entre les deux transceiver de part et d’autre du segment. Lorsqu’il n’y a pas de trame, le transceiver envoie sur la paire émission une succession de signaux de test (*link test pulse*). De l’autre côté du segment ce signal est détecté par le transceiver sur la paire de réception. Ce transceiver vérifie ainsi l’intégrité de la ligne ou plutôt de ce qui est pour lui la paire de réception. La liaison est considérée comme défectueuse lorsque aucun signal est reçu dans un intervalle de 50 à 150 ms. Pour que cette liaison soit à nouveau active, deux à dix *link test pulse* consécutifs doivent être reçus. Sur la plupart des transceivers, un voyant permet de vérifier l’état de la ligne grâce à cette fonction *link detection*.

Auto-partition. Le hub dispose aussi d’une autre fonction de contrôle qui permet d’isoler des segments défectueux. L’auto-partition provoque l'arrêt de toute transmission entre un segment en faute et tous les autres ports du hub. Par contre, le trafic de ses autres ports continue d'être transmis sur le segment défectueux. Un segment est considéré en faute soit lorsque, plus de trente collisions consécutives ont été observées sur le segment, soit lorsqu’il y a une collision permanente. Le hub doit, lorsqu'il constate la disparition du défaut, rétablir la connexion du segment. Une cause classique qui justifie la fonction d’auto-partition sur un segment coaxial neuf est l'oubli de la terminaison de 50 ohms à l'extrémité du segment.

Interconnexion de hubs

Si le nombre de ports sur un hub n'est pas suffisant, il peut être étendu en cascadant plusieurs hubs. Dans un réseau composé de hubs cascadés, le cordon reliant un hub à un autre est considéré comme un segment. Les mêmes règles d'interconnexion de hubs (= répéteur) et de segments comme dans les réseaux 10Base-5 et 10Base-2 s'appliquent. Un chemin entre deux stations ne doit pas traverser plus de 4 répéteurs. Un exemple d'une telle configuration est montré sur la Figure 31.

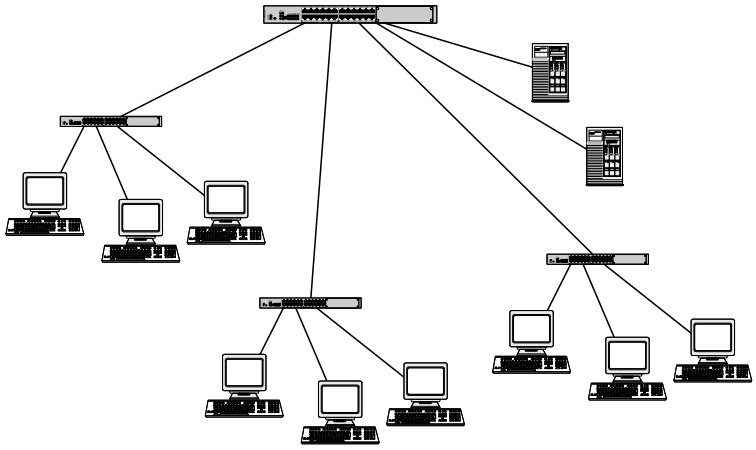


Figure 31: Configuration d'un réseau en hubs cascadés

La distance maximale entre deux stations dans un réseau 10Base-T est donc de 500 m. Si l'on veut relier des stations encore plus éloignées, on peut utiliser des segments 10Base-5 comme épine dorsale (Figure 32).

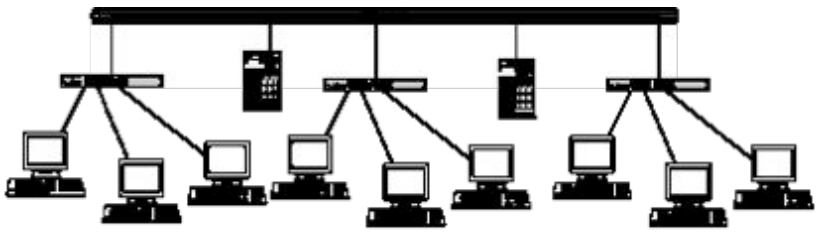


Figure 32: Configuration avec un segment 10Base-5 comme épine dorsale

4.3.2 FastEthernet

L'émergence de nouveaux services téléinformatiques et du multimédia stimulant la demande de plus haut débit de nombreuses études ont été menées depuis le début des années 90 pour amener à maturité de nouveaux standards de protocoles Ethernet à 100Mb/s. La technique d'accès est la même que dans la version Ethernet 10 Mb/s, mais à une vitesse multipliée par 10. Les trames transportées sont identiques.

Plusieurs normes ont été définies, selon le support physique utilisé :

- 100Base-TX (1995) : utilise deux paires torsadées d'un câble UTP catégorie 5 (ou deux paires blindées STP).

- 100Base-T4 (1995) : requiert quatre paires d'un câble UTP des catégories 3, 4 ou 5.
- 100Base-T2 (1997) : utilise deux paires torsadées d'un câble UTP catégorie 3 ou plus haute.
- 100Base-FX : requiert deux fibres optiques multimodes.

On constate que les câbles coaxiaux ne sont plus supportés pour les réseaux FastEthernet.

Les produits supportant la norme 100Base-TX ont été les premiers à apparaître sur le marché. Des produits supportant 100Base-T4 sont venu peu de temps après, mais trop tard pour contester la place à 100Base-TX. Outre cela, 100Base-T4 ne supportait pas le mode full-duplex, contrairement à 100Base-TX. La norme 100Base-T2, qui n'a été approuvée qu'en 1997, est arrivé beaucoup trop tard pour susciter l'intérêt du marché. En effet, aucun fournisseur d'équipement n'a implémenté cette norme.

De ce fait, seulement les normes 100Base-TX et 100Base-FX sont utilisées en pratique.

La couche MAC FastEthernet

La couche MAC du 100BASE-TX est presque identique à celle de l'Ethernet à 10Mb/s. Lors de la standardisation d'Ethernet à 10 Mb/s l'IEEE avait spécifié les paramètres de sa couche MAC en faisant abstraction de la vitesse. Il a donc suffi de réduire la durée de transmission de chaque bit d'un facteur de 10 pour découpler la vitesse théorique du 100Base-T. Et grâce à cette indépendance par rapport à la vitesse, toutes les fonctions de cette couche MAC Ethernet à 10 Mb/s sont conservées dans la norme 100Base-TX.

Cette absence de modification est très importante et permet de passer des 10Mb/s à 100 Mb/s sans changement au niveau des couches logiciels.

Le *délai aller-retour maximal* n'est pas changé lorsque celui-ci est exprimé en temps-bit. Par contre ramené à l'échelle temps est divisé par 10. Naturellement le fait de garder les mêmes dimensions de trame ainsi que tous les autres paramètres (exprimés en temps-bit) implique comme corollaire que l'étendue physique du réseau est aussi divisée approximativement par 10. Elle est d'à peu près 200 m au lieu et place de plus de 2 km dans les réseaux à 10 Mb/s.

La Table 8 montre les paramètres de base de la couche MAC.

Table 8: Paramètres de la couche MAC de FastEthernet

Paramètre	
Débit de transmission	100 Mb/s
Délai aller-retour maximal	512 temps bit (= 5.12 μs)
Longueur du signal jam	32 bits
Interframe gap	0,96 μs
Taille minimale d'une trame	64 octets

4.3.2.1 100Base-TX

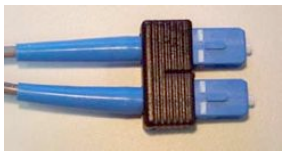
Le câblage et les connecteurs de 100Base-TX sont similaires à la norme 10Base-T, à la différence près que des câbles UTP de catégorie 5 sont à utiliser. La configuration d'un réseau 100Base-TX est en étoile, avec un hub au centre. La longueur maximale d'un segment est de 100 m.

4.3.2.2 100Base-FX

La norme100Base-FX utilise des fibres optiques multimodes pour la transmission des signaux. La 2^{e} fenêtre de transmission est utilisée (longueur d'onde de1300 nm). Le câble comprend deux fibres : une pour l'émission et l'autre pour la réception. Le croisement des fonctions d'émission et de réception doit être réalisé par le câble.

Les connecteurs prévus par la norme sont (Figure 33) :

- Connecteur duplex SC (recommandé)
- Connecteur MIC
- Connecteur ST



Connecteur duplex SC

Connecteur MIC

Connecteur ST

Figure 33: Connecteurs optiques

La longueur maximale d'un segment 100Base-FX est de 412 m.

4.3.2.3 Interconnexion de segments FastEthernet

La norme définit deux types de hubs (ou répéteurs) pour interconnecter des segments FastEthernet.

Répéteurs classe I. Un tel répéteur est utilise pour interconnecter des segments FastEthernet avec une signalisation différente (comme p. ex. 100Base-TX/FX et 100Base-T4). À cause de la conversion entre les segments, ces répéteurs introduisent un délai supplémentaire. Selon la norme, un seul répéteur classe I peut être dans le chemin entre deux stations.

Répéteur classe II. Ces répéteurs peuvent interconnecter des segments FastEthernet du même type, donc sans conversion de signalisation. Un tel répéteur peut interconnecter des segments 100Base-TX et 100Base-FX mais non 100Base-TX/FX avec 100Base-4. Leur délai interne étant plus faible, jusqu'à deux répéteurs classe II peuvent être traversés par une transmission entre deux stations.

Le calcul de l'étendue maximale d'un domaine de collision FastEthernet est basé sur les délais maximum introduits par chaque élément du réseau. La Table 9 résume les

résultats. Pour des raisons de simplicité seulement l'interconnexion de segments du même type est considérée.

Table 9: Etendue maximale de réseaux FastEthernet

Configuration	100Base-TX	100Base-FX
Longueur maximale d'un segment	100 m	412 m
Réseaux avec un répéteur classe I	200 m	272 m
Réseaux avec un répéteur classe II	200 m	320 m
Réseaux avec deux répéteurs classe II	205 m	228 m

On remarque que l'emploi de répéteurs ou de hubs dans un réseau 100Base-FX ne permet pas d'augmenter l'étendue du réseau mais seulement de connecter un nombre de stations plus élevé.

4.3.3 Gigabit-Ethernet

Le Gigabit Ethernet est la dernière évolution du standard Ethernet. Le Gigabit Ethernet basé sur la norme 802.3 peut être utilisé soit au travers la fibre ou à travers le fil de cuivre. Gigabit Ethernet offre un débit maximal de 1000 Mb/s et se présente comme une extension de la technologie Ethernet à 10 ou 100 Mb/s.

Les différentes solutions normalisées sont les suivantes :

1000base-LX (*long wavelength*). Ce mode utilise une paire de fibre optique avec une longueur d'onde élevée (1300 nm). Un segment peut couvrir des distances plus longues, allant jusqu'à 5000 m. Il se prête comme épine dorsale (*backbone*) dans un bâtiment ou sur un campus.

1000base-SX (*short wavelength*). Similaire à 1000Base-LX, une paire de fibres optiques est utilisée. Cependant, la transmission se fait sur une longueur d'onde plus courte, ce qui la distance de la transmission sur un segment à environ 500 m. L'avantage de 1000Base-SX par rapport à 1000Base-LX est le prix inférieur des transceivers. Cette technologie est bien adaptée pour le câblage d'un étage.

1000base-T (IEEE 802.3ab). Ce mode est le dernier qui a été approuvé. Il utilise quatre paires UTP de catégorie 5 pour la transmission. Le débit élevé nécessite des méthodes de codage sophistiquées. 1000Base-T permet une longueur des segments jusqu'à 100 m.

Les différentes solutions du Gigabit Ethernet peuvent s'interconnecter par l'intermédiaire d'un répéteur ou d'un hub. Un seul type de répéteur est défini. Pour respecter le délai maximum aller-retour de 512 ns, un seul répéteur ou hub est permis dans un domaine de collision.

La Table 10 résume les paramètres des différentes technologies Gigabit-Ethernet.

Table 10: Paramètres des technologies Gigabit-Ethernet

Technologie	Support physique	Longueur d'un segment	Etendue max. avec un répéteur/hub
1000Base-T	4 paires d'un câble UTP cat. 5	100 m	200 m
1000Base-LX	Fibres multi-mode 62,5 μm	550 m	220 m
	Fibres multi-mode 50 μm	550 m	

	Fibres mono-mode 10 μm	5000 m	
1000Base-SX	Fibres multi-mode 62,5 μm	275 m	
	Fibres multi-mode 50 μm	500 m	

4.3.3.1 La couche MAC de Gigabit-Ethernet

L'IEEE a beaucoup insisté pour que Gigabit Ethernet half-duplex avec la stratégie d'accès CSMA/CD soit implémenté. Ainsi plusieurs stations pourront partager un même port et donc une bande passante de 1 Gb/s.

Le problème essentiel lors de la mise en oeuvre de l'algorithme CSMA/CD dans Gigabit Ethernet c'est la longueur minimale de la trame. En effet pour qu'une station puisse détecter les collisions, il faut qu'elle puisse encore émettre pendant tout le temps de vulnérabilité. Du fait que dans le Gigabit Ethernet le temps de transmission est si élevé un problème de taille de trame apparaît. Pour être compatible avec les autres versions d'Ethernet, ce qui est un principe de base, la taille de la trame émise doit se situer entre 64 et 1500 octets. Les 64 octets, c'est-à-dire 512 bits, correspondent à un temps d'émission de 512 ns. Pour qu'une station émettrice puisse détecter une éventuelle collision, la taille maximale doit être choisie de telle manière que le temps aller-retour d'un signal soit inférieur à temps de transmission minimal. Pour un temps d'émission de 512 ns, la longueur maximale du support physique est de 20 m. Dans les faits, avec un hub de rattachement et les portions de câble jusqu'aux coupleurs, la distance maximale est ramenée à quelques mètres. Pour pallier cette difficulté et permettre des distances plus grandes, Gigabit Ethernet exploite la technique *Carrier Extension.* Cette technique ne change pas la taille de la trame, mais allonge le temps de transmission, en garantissant ainsi un temps équivalent à une trame de **512 octets au minimum**. Le coupleur ajoute des octets de bourrage qui sont ensuite enlevés par le coupleur récepteur.

S'il s'agit là d'une bonne solution pour agrandir le réseau Gigabit, le débit utile est toutefois très faible si toutes les trames à transmettre ont une longueur de 64 octets, un huitième de la bande passante étant utilisé dans ce cas.

Une autre modification de la couche MAC pour Gigabit-Ethernet est le *frame bursting*. Cette option permet à une station de transmettre jusqu'à 65536 bits (donc plus de 5 trames de taille maximale) sans donner la possibilité de transmission aux autres stations. L'*interframe gap*, qui doit être respecté normalement entre les émissions des trames, est rempli avec des bits d'extension qui permettent aux autre stations de détecter la transmission en cours.

La résume les paramètres de la couche MAC dans Gigabit-Ethernet.

Table 11: Paramètres de la couche MAC de FastEthernet

Paramètre	
Débit de transmission	1 Gb/s
Délai aller-retour maximal	4096 temps bit (= 4,1 μs)
Longueur du signal jam	32 bits
Interframe gap	96 ns
Taille minimale d'une trame	512 octets
Taille maximale d'un *frame burst*	65536 bits

4.3.4 Auto-négociation

Dans les sections précédentes nous avons vu que plusieurs normes Ethernet utilisent des câbles UTP avec des connecteurs RJ-45 comme média de transmission. Il est donc tout à fait possible que deux cartes réseaux connectées aux bouts d'un segment UTP implémentent des normes différentes. La procédure d'auto-négociation permet la détection des capacités d'un équipement partenaire sur une liaison UTP et d'établir configuration automatique des équipements.

L'auto-négociation fonctionne sur un câble UTP (et non pas STP ou fibre optique), doté de 8 conducteurs (4 paires). Elle est spécifiée comme option pour les réseaux 10Base-T, 100Base-TX et 100Base-T4. Pour les réseaux 100Base-T2 et 1000Base-T elle est obligatoire. Pour être compatible avec les équipements qui ne disposent pas de cette procédure, elle utilise des trains d'impulsions similaires à ceux déjà utilisés par la fonction *link detection* (voir la section Hubs, page 38).

L'auto-négociation permet aux cartes réseaux

- d'annoncer le mode Ethernet implémenté et des fonctionnalités optionnelles à une carte à l'autre bout du segment,
- de confirmer la réception et la compréhension des modes que les deux cartes supportent,
- de refuser un mode non supporté,
- de configurer le mode le plus approprié que les deux cartes supportent.

Si plusieurs modes sont possibles entre deux cartes, le choix se fait selon la priorité de chaque mode, définie dans la norme (Table 12).

Table 12: Priorité des modes Ethernet dans l'auto-négociation

Mode	Priorité
1000Base-T full-duplex	9
1000Base-T half-duplex	8
100Base-T2 full-duplex	7
100Base-TX full-duplex	6
1000Base-T2 half-duplex	5
1000Base-T4 half-duplex	4
1000Base-TX half-duplex	3
10Base-T full-duplex	2
10Base-T half-duplex	1

L'auto-négociation utilise une séquence d'impulsions de test de liens modifie dans laquelle les impulsions normales sont remplacées par des rafales d'impulsions rapides (FLPs, *Fast Link Pulses*), comme montrées sur la Figure 34. Une rafale comprend 33 positions dont 16 représentent des bits 0 ou 1, selon la présence ou non d'une impulsion. Ainsi il est possible de coder les modes supportés d'une carte réseau et d'autres informations. Une carte réseau qui ne répond pas au rafales FLP et ne renvoie que des séquences de test de liens normales est considérée comme supportant le mode 10Base-T half-duplex.

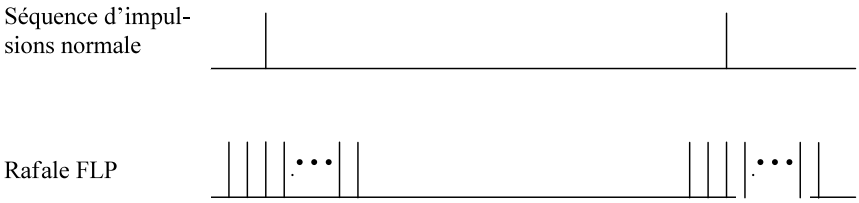


Figure 34: Rafales FLP de l'auto-négociation

Les modes Gigabit-Ethernet basés sur fibres optiques (1000Base-LX/SX) utilisent eux aussi une procédure d'auto-négociation afin de configurer la transmission full-duplex ou half-duplex ainsi que la direction du contrôle de flux.

5 Token Ring (anneau à jeton)

L'anneau à jeton est le fruit d'années de recherches et d'expérimentations menées principalement par les scientifiques du laboratoire IBM de Zürich. Le travail a été poursuivi par les ingénieurs et programmeurs du *Research Triangle Park*. C'est ce centre de recherche qui s'est chargé du développement du logiciel et du matériel nécessaire à l'implémentation des premiers produits Token Ring.

Dès le départ, ce réseau local a été défini par IBM comme un réseau pouvant relier des machines de toutes dimensions : micro-ordinateurs et ordinateurs départementaux ou centraux. On admet, par ailleurs, que l'anneau à jeton, réputé coûteux, se prête davantage à des transactions temps réel, tandis qu'Ethernet convient plutôt à des échanges volumineux (documents, textes ou graphiques, CAO, etc.). Un anneau physique est sans imprévu et possède une limite maximale de temps d'accès au canal de transmission parfaitement contrôlable. C'est principalement pour ces raisons qu'IBM a choisi un anneau comme offre de produit réseau LAN et que IEEE a inclus dans ses normes un anneau à jeton : la norme IEEE 802.5 (1985).

L'apparition de la norme IEEE 802.5 a ouvert le système Token Ring aux produits non-IBM, et l'on trouve sur le marché une grande variété de cartes adaptateur pour l'anneau à jeton. De même, de nombreux systèmes d'exploitation supportant le Token Ring sont disponibles.

D'autres normes basées sur le passage d'un jeton (*token*) existent. Les réseaux IEEE 802.4 (bus à jeton, *Token Bus*) utilise aussi la méthode du jeton, mais sur un bus et non pas sur un anneau. Le HSTR (*High-Speed Token Ring*) est une évolution de la technologie de Token Ring, travaillant à une vitesse jusqu'à 100 Mb/s. FDDI (*Fiber Distributed Data Interface*) est une technologie MAN à 100 Mb/s, utilisant deux anneau pour offrir une protection contre des pannes.

Cette section présente principalement la norme Token Ring, étant la technologie la plus importante parmi les réseaux à jeton. Les autres technologies n'ont souvent qu'un intérêt historique ou un domaine d'application très spécifique. Pour les lecteurs intéressés, un paragraphe sur les réseaux FDDI conclut la section.

5.1 Structure des réseaux Token Ring

Les réseaux de transmission en structure de boucle ou d'anneau physique sont utilisés depuis de nombreuses années aussi bien par des réseaux LAN que par des réseaux MAN ou WAN. L'ingénierie d'un anneau physique repose totalement sur une technologie numérique, contrairement aux réseaux 802.3, qui utilisent des composants analogiques pour assurer la détection des collisions.

La Figure 35 illustre la structure d'un réseau Token Ring.

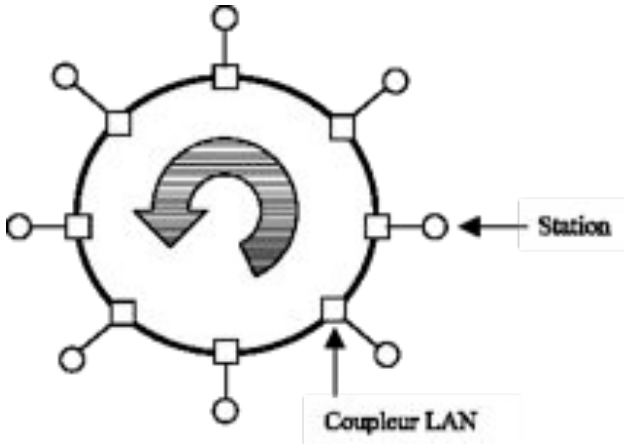


Figure 35: Un réseau Token Ring

Un anneau physique n'est pas un simple réseau à diffusion mais une succession de liaisons point à point reliées aux contrôleurs LAN des stations. Les liens point à point forment une structure circulaire. Chaque station joue le rôle d'un répéteur fournissant l'amplification nécessaire aux signaux. Un bit arrivant à l'entrée d'un coupleur est copié dans une mémoire tampon de 1 bit, avant d'être réémis sur le tronçon aval du réseau. Lorsqu'il est en mémoire, le bit peut être inspecté et sa valeur modifiée avant qu'il soit réémis.

Sur un anneau à jeton, une trame particulière appelée jeton (token) circule en permanence lorsque les stations n'ont rien à transmettre. Le jeton comporte 24 bits (3 octets). Pour un fonctionnement correct, l'anneau doit présenter un temps de propagation tel qu'il est suffisant pour contenir un jeton complet. Si le débit sur l'anneau est de 4 Mb/s, l'anneau doit avoir un temps de propagation de 24 bits / 4 Mb/s = 6 μs. Ceci semble un délai très court mais imaginez une paire torsadée dans laquelle la vitesse de propagation est 0,59 fois la vitesse de la lumière. La formule suivante permet de calculer la taille de l'anneau avec un temps de latence de 6 μs :

Taille de l'anneau = Temps de propagation x Vitesse de propagation sur le média
= 6 μs x 0,59 x 300'000 km/s
= 1062 m.

Ainsi, la taille minimale de l'anneau devrait être de 1 km ! C'est très long, surtout si vous désirez installer plusieurs stations dans une pièce. Pour cette raison, une station spéciale désignée comme moniteur actif ajoute un buffer de 24 bits sur l'anneau pour augmenter artificiellement le temps de propagation autour de l'anneau.

5.1.1 Câblage physique

Dans un fonctionnement normal de l'anneau, une station peut être éteinte. Mais que se passe-t-il si le jeton arrive dans une station éteinte ? En fait, les réseaux Token Ring sont **câblés en étoile avec un hub central**. Chaque connexion entre le hub et une station est contrôlée par un relais situé dans le hub. Sur la Figure 36, les relais sont maintenus ouverts par les stations en fonctionnement. Quand une station est éteinte, le relais se ferme. Ce mécanisme est appelé *shuntage*. Il permet aussi de déconnecter une station défectueuse, qui pourrait mettre en danger le fonctionnement correct de l'anneau.

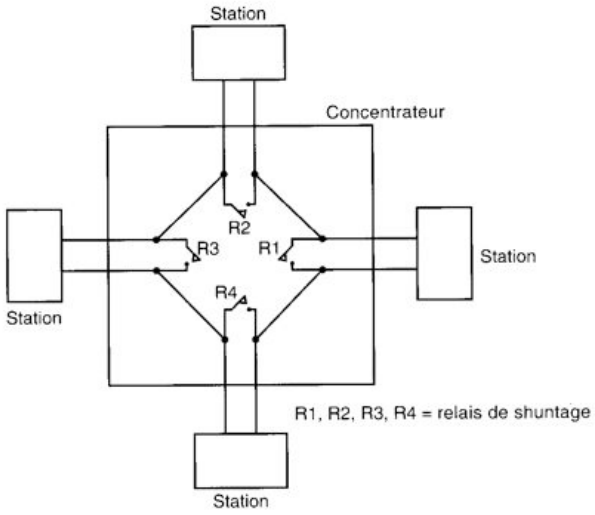


Figure 36: Câblage d'un réseau Token Ring

5.2 Le protocole MAC 802.5

Le fonctionnement de base du protocole MAC 802.5 est très simple. Quand il n'y a aucun trafic sur l'anneau, un jeton comptant 3 octets y circule en permanence attendant qu'une station désirant transmettre une trame le capture et modifie le bit « Token » du jeton, transformant ainsi le jeton libre en une trame normalement constituée prête à transmise sur le réseau (Figure 38).

Dans des conditions de fonctionnement normales, le premier bit de la trame est déjà de retour à la station émettrice alors qu'une bonne partie de la trame reste encore à transmettre. Seul un anneau très long est en mesure de contenir complètement une trame, même courte. En conséquence, une station qui transmet une trame doit la retirer de l'anneau tout en continuant à transmettre la suite de la trame. Comme l'illustre la Figure 37, cela signifie que les bits qui ont effectué un tour complet reviennent à la station émettrice, qui les retire de l'anneau. Ceci permet à la station émettrice de vérifier que la trame a été correctement reçue par le destinataire.

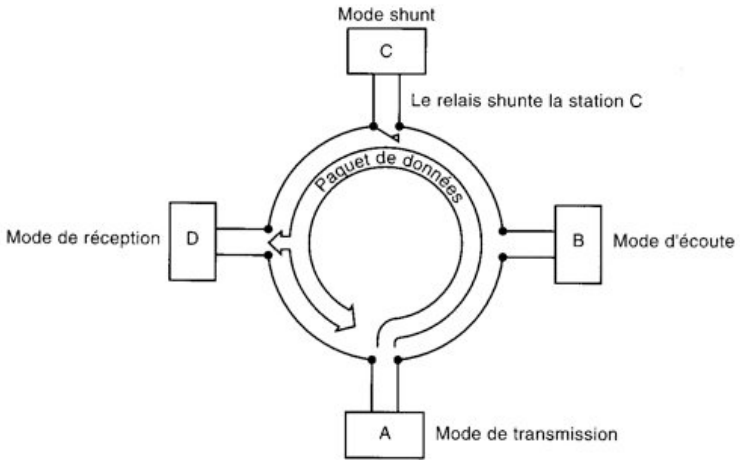


Figure 37: Modes des stations dans un réseau Token Ring

Temps de maintien du jeton. Chaque station peut garder le jeton en sa possession pendant une durée maximale de 10 ms, appelée *temps de maintien du jeton*, à moins qu'une autre valeur ne soit spécifiée sur une installation particulière. S'il reste suffisamment de temps après la transmission d'une trame pour en transmettre une autre, cette transmission pourra alors s'effectuer. Lorsque toutes les trames en attente ont été transmises ou lorsque la durée maximale permise est écoulée, la station doit cesser son processus d'émission et générer un nouveau jeton.

5.2.1 Format des trames Token Ring

Le format des trames Token Ring est montré sur la Figure 38.

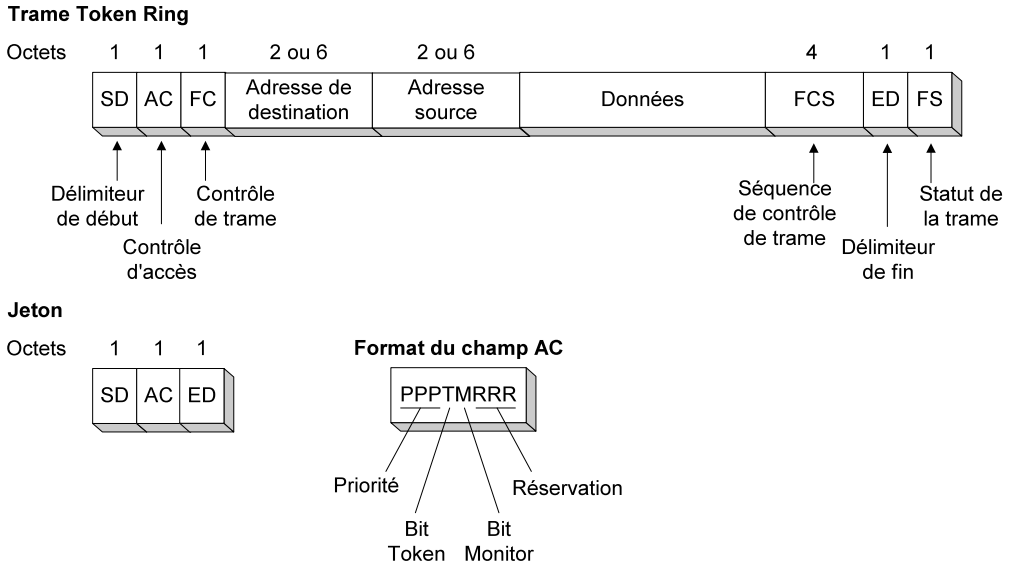


Figure 38: Format des trames Token Ring

Les champs « Délimiteur de début » et « Délimiteur de fin » marquent le début et la fin de la trame. Le champ « Contrôle d'accès », que nous décrivons plus bas, contient le bit définissant le jeton et 7 autres bits, dont un bit de supervision (le bit « Moniteur »), 3 bits de priorité et 3 bits de réservation.

Le champ « Contrôle de trame » identifie des trames spéciales. Sa fonction est décrite dans la Section 5.2.3. Les deux champs suivants, Adresse de destination et Adresse source, sont les mêmes que ceux des trames Ethernet. Ils sont suivis par le champ Données qui peut être aussi long que la durée du compteur « temps de maintien du jeton » le permet. Le champ FCS permet le contrôle d'erreur des trames comme dans les réseaux Ethernet.

Un champ aux fonctions intéressantes, porte le nom de « Statut de la trame ». Sa fonction et décrite dans la section suivante.

Transmission de datagrammes IP. Le standard IEEE 802.5 utilise la trame LLC pour encapsuler les données des couches supérieures. L'en-tête SNAP est utilisé pour envoyer les datagrammes IP, comme montré sur la Figure 39.

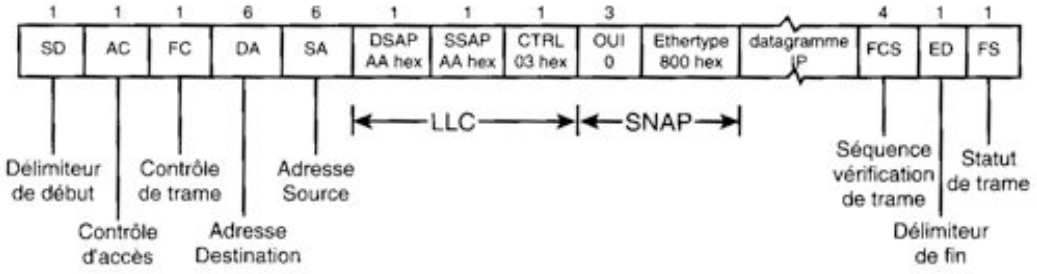


Figure 39: Transmission d'un datagramme IP dans une trame Token Ring

5.2.2 Transmission d'une trame

Une station d'un réseau Token Ring opère dans l'un des quatre modes suivants :

- mode de transmission
- mode d'écoute
- mode « déconnecté »
- mode de réception.

La Figure 37 montre quatre stations opérant chacune dans un mode différent. La station A transmet. Pour entrer dans ce mode, elle saisit un jeton libre. Le jeton possède un bit appelé le bit T. La valeur de ce bit détermine l'état du jeton. Il est libre si le bit T est à 1. La station qui émet modifie ce bit. Elle le met à 0, ce qui indique qu'il est occupé, et transmet ses données. La station A envoie ses données à la station D. Le champ d'adresse de destination contient l'adresse de D, tandis que le champ d'adresse source contient l'adresse de A.

La station B est en mode d'écoute. Elle vérifie le champ d'adresse de destination pour savoir si les données lui sont destinées. Comme la trame est envoyée à la station D, la station B reste en mode d'écoute. Dans ce mode, la station copie les données entrantes dans le câble de sortie.

La station C a été éteinte et se trouve en mode « déconnecté ». Les données passent directement sans traverser la station C.

La station D examine le champ d'adresse de destination et découvre que les données lui sont destinées. Elle entre en mode de réception. Dans ce mode, la trame est copiée dans la mémoire de la station et envoyée aussi sur l'anneau.

Plusieurs bit du champ « Statut de la trame » sont modifiés pour indiquer la réception des données. La station A reçoit la trame de données envoyée et examine les drapeaux. Ces drapeaux jouent le rôle d'accusés de réception. La station émettrice vérifie ainsi si la trame a été correctement reçue par la station D.

Statut de la trame

La Figure 40 montre les bits du champ « Statut de la trame ».

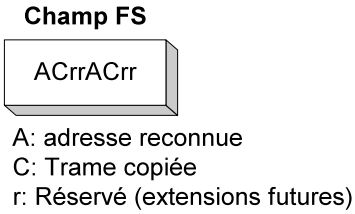


Figure 40: Format du champ « Statut de la trame »

Il convient de noter que les drapeaux A et C sont dupliqués dans le champ de statut de la trame (FS) pour pallier le fait qu'ils ne soient pas protégés par le FCS.

Le destinataire positionne les bits A du champ FS à 1. Si le coupleur copie la trame pour la station, il positionne également les bits C à 1. Une station peut être dans l'impossibilité de copier entièrement la trame par manque de place en mémoire de réception ou parce qu'elle est entachée d'erreurs de transmission (FCS est incorrecte). Quand l'octet Statut de trame revient à la station émettrice, celle-ci examine les paires de bits A et C. Trois combinaisons sont possibles

1. A = 0 et C = 0 le destinataire n'est pas actif
2. A = 1 et C = 0 le destinataire est actif mais la trame n'a pas été acceptée.
3. A = 1 et C = 1 : le destinataire est actif et la trame a été copiée (donc acceptée).

Cette disposition fournit un accusé de réception automatique pour chaque trame. Si une trame n'est pas copiée mais que le destinataire est actif l'émetteur de la trame peut tenter de la retransmettre un peu plus tard.

Le champ « Délimiteur de fin » contient un bit dénommé E, pour erreur. Il sera positionné par tout coupleur de réseau qui détectera une erreur au moment du calcul de la FCS. Il possède également un bit qui permet d'indiquer si la trame est la dernière d'une suite logique de trames, en quelque sorte une espèce de fin de séquence ou de fichier.

Priorités de transmission

Le protocole 802.5 est doté d'un mécanisme d'accès élaboré pour la gestion des trames prioritaires. Le jeton comporte deux séquences de bit dans le champ « Contrôle d'accès » :

- une séquence « priorité »
- une séquence de réservation.

Chaque séquence contient trois bits. Huit priorités sont définies (de 0 à 7). La séquence de réservation est mise à 0 par la station qui transmet. Si une station demande une priorité d'accès, elle peut placer une valeur correspondant à la priorité dans les bits de réservation. Après réception de la trame envoyée par la station émettrice, elle copie la valeur de la réservation dans la séquence « priorité » du nouveau jeton qui est généré. Le jeton possède maintenant la priorité demandée. Seules les stations possédant une priorité supérieure ou égale peuvent accéder à ce jeton.

5.2.3 Gestion de l'anneau

Chaque anneau à jeton est doté d'une station qui joue un rôle particulier, celui de moniteur, qui consiste à superviser la circulation du jeton et des trames sur l'anneau. Si le moniteur vient à défaillir, il est remplacé immédiatement par une autre station, toutes les stations en ayant la capacité. En cas de candidatures multiples, un protocole (basé sur l'ordre des adresses MAC) désigne l'une des stations comme moniteur. Lorsque le moniteur assume sa fonction, lui seul est responsable de la gestion de l'anneau.

La gestion de l'anneau se fait à l'aide de trames spéciales, les trames de commande. Elles portent des codes particuliers dans le champ « Contrôle de trame », comme montré dans la Table 13.

Table 13: Codes des trames de commande

Code dans le champ FC	Nom de la trame	Objet de la trame
0000 0000	Test d'adresse	Teste si deux stations ont même adresse.
0000 0010	Alarme	Localisation d'une station défaillante
0000 0011	Demande du jeton	Tentative de devenir moniteur
0000 0100	Purge	Initialisation de l'anneau
0000 0101	Moniteur présent	Utilisé périodiquement par le moniteur pour signaler sa présence
0110 0111	Moniteur potentiel	Signale la présence d'un moniteur potentiel.

Les trames de commande sont utilisées pour résoudre les problèmes qui peuvent apparaître dans le réseau.

Panne du moniteur. Au moment de l'activation de la première station de l'anneau ou quand l'une des stations constate qu'il n'y a pas de moniteur, elle peut transmettre la trame de commande « Demande de jeton ». Si cette trame effectue une rotation sur l'anneau sans que d'autres trames similaires ne soient passées au niveau de la station émettrice, celle-ci devient le moniteur de l'anneau.

Trame orpheline. Une trame orpheline peut apparaître lorsque l'anneau est très long et que les trames sont courtes. Pour cela, il suffit que la station ait fini d'émettre sa trame avant que le début de celle-ci ne lui revienne et qu'elle l'ait retirée de l'anneau (p.ex. éteinte). Si rien n'est fait la trame tournera indéfiniment et aucun nouveau jeton ne sera généré. Une trame orpheline est détectée par l'intermédiaire du bit moniteur du champ Contrôle d'accès. Normalement, le bit moniteur est positionné à 0 au moment de la génération du jeton; il est positionné à 1 par le moniteur lorsqu'il le voit passer. Dans tous les cas les jetons ne doivent pas se représenter au moniteur. S'ils se représentent c'est que quelque chose n'a pas fonctionné ; il faut alors purger l'anneau et injecter un nouveau jeton, ce que fait le moniteur.

Perte du jeton. Pour contrôler la perte du jeton, le moniteur est doté d'un compteur de temps dont la valeur est légèrement supérieure à la durée maximale du temps de maintien du jeton par une station, à laquelle on ajoute la durée d'une rotation sur l'anneau dans sa configuration maximale. Si ce compteur expire, c'est qu'il n'y a plus de jeton sur l'anneau, et le moniteur purge l'anneau et y injecte un nouveau jeton.

Trame erronée. Quand le moniteur reconnaît une trame de format invalide, il « ouvre » l'anneau pour l'extraire. Il émet ensuite une séquence de purge et injecte un nouveau jeton avant de retourner en mode écoute.

Localisation de coupures de câble. La localisation des coupures de câbles est une opération de supervision qui n'est pas assurée par le moniteur. Quand une station se rend compte que son voisin en amont cesse de lui faire parvenir des signaux, elle transmet une trame d'alarme (BCN, *beacon*) sur l'anneau contenant l'adresse de la station présumée défaillante. Lorsque cette station reçoit plusieurs de ces trames d'alarme, elle se déconnecte temporairement de l'anneau et se réinitialise pour essayer de corriger l'erreur. Si cela n'a pas d'effet, l'administrateur du réseau doit intervenir manuellement.

5.2.4 Variantes Token Ring

L'IEEE 802.5 indique les options d'implémentation de Token Ring à 1 Mb/s, 4 Mb/s et 16 Mb/s. Les trois options peuvent être réalisées sur des câbles UTP.

Early Token Release. Le fonctionnement d'un réseau Token Ring à 16 Mb/s est différent des autres variantes. Dans le cas d'un réseau à 16 Mb/s, le coupleur rend immédiatement le jeton, contrairement aux réseaux à 4 Mb/s, où le coupleur rend le jeton après que la trame a effectué un tour de la boucle. Il y a donc une libération anticipée du jeton, qui permet à plusieurs trames de circuler simultanément dans l'anneau. Ainsi, la capacité du réseau peut être mieux exploitée.

Token Ring commuté. Comme pour Ethernet, une amélioration des réseaux Token Ring passe par la commutation. Dans un premier temps, on améliore la quantité d'informations transmises en divisant les réseaux Token Ring en sous-réseaux reliés à des ports d'un commutateur. Le cas extrême est atteint lorsque chaque coupleur est relié directement au commutateur par une boucle simple qui ne relie que lui.

5.2.5 FDDI

Le concept FDDI (*Fiber Distributed Data Interface*) définit un réseau local ou métropolitain performant, pouvant véhiculer des données à haut débit (100 Mb/s) avec une administration de réseau intégrée. Les avantages de la fibre optique, tels que sa largeur bande passante, son immunité aux perturbations électromagnétiques ou sa faible atténuation, ont poussé à une normalisation de FDDI, avec la fibre optique comme support physique. On s'est aperçu depuis quelques années que FDDI pourrait très bien se satisfaire de la paire torsadée pour des distances allant jusqu'à une centaine de mètres. Cette solution a permis de réduire les coûts d'installation et contribué à une augmentation notable du nombre de réseaux FDDI installés dans le monde. Le réseau FDDI-II est le successeur de FDDI. Il a été modifié pour prendre en compte notamment des trafics de données isochrones, comme par exemple des canaux de voix numérisée. Nous présentons FDDI par la suite.

FDDI fut considéré pendant un temps comme le réseau LAN de nouvelle génération dont l'entreprise avait besoin. En réalité, il n'a pas atteint le succès escompté. Il s'est tout simplement cantonné à jouer un rôle de réseau fédérateur de LAN à bas débit. La raison du demi-échec de FDDI est liée au fait que la gestion des stations FDDI est compliquée ; elle nécessite des composants complexes et coûteux. Le coût substantiel des composants FDDI à mettre dans chaque station connectée au réseau n'a pas

encouragé les fabricants de stations de travail à imposer FDDI comme standard pour les réseaux LAN à haut débit. C'est ainsi que FDDI n'a pas réussi à se faire la place attendue sur le marché.

5.2.5.1 Topologie et fonctionnalités des réseaux FDDI

Les réseaux FDDI reposent sur une topologie en double anneau contrarotatif, ce qui offre un très bonne tolérance aux pannes.

Il existe trois classes d'équipement :

- la classe A, connectée au double anneau,
- la classe C, composée des concentrateurs,
- et la classe B, qui regroupe les équipements connectés à un seul des anneaux par un concentrateur.

Cette topologie est illustrée à la Figure 41. Cette structure permet de connecter 500 stations de type A et C ou 1000 stations de type B sur une distance totale de 100 km.

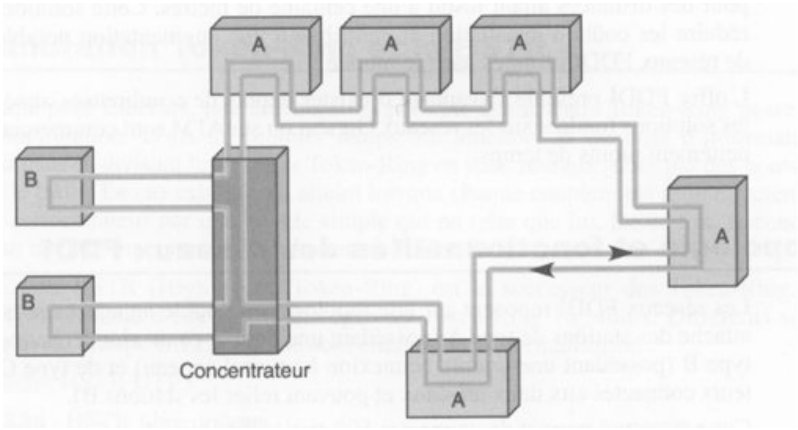


Figure 41: Topologie en double anneau des réseaux FDDI

Le support physique consiste en de la fibre optique multimode, mais d'autres possibilités sont acceptables, notamment de la fibre optique en monomode, qui porte la distance entre deux nœuds à 60 km au lieu de 2 km.

Tolérance aux pannes. La tolérance aux pannes constitue l'un des grands avantages d'un réseau FDDI. En cas de coupure d'un des anneaux, le réseau utilise le deuxième anneau. En cas de coupures multiples, le réseau se reconfigure automatiquement en un seul anneau, comme illustré à la Figure 42, ou, si nécessaire, en plusieurs sous-réseaux.

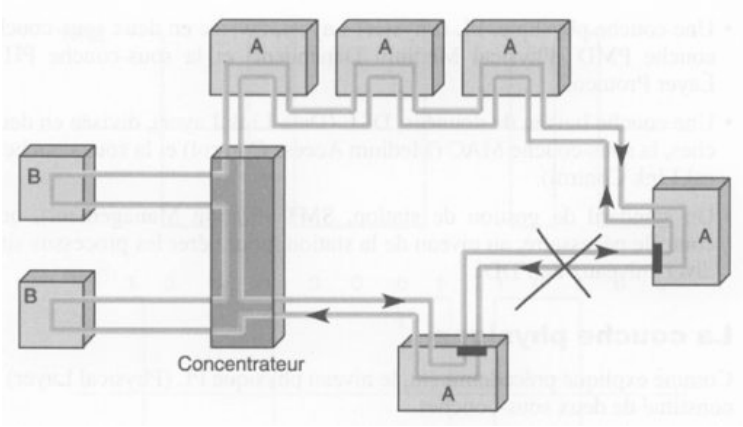


Figure 42: Configuration de repli en cas de coupure

Méthode d'accès. La méthode d'accès utilise un jeton temporisé. FDDI offre les deux classes de service suivantes :

- Service synchrone, qui correspond aux applications nécessitant une bande passante garantie et/ou un délai de transmission déterminé.
- Service asynchrone, qui satisfait aux contraintes de trafic en créant une certaine quantité de bande passante partagée par toutes les stations qui utilisent ce service.

Afin d'offrir un service satisfaisant au trafic synchrone, le temps de rotation du jeton est contrôlé, c'est-à-dire que le temps total mis par le jeton pour parcourir tout le réseau doit rester en dessous d'un seuil fixé par les applications utilisant le réseau.

De façon optionnelle, on distingue plusieurs niveaux de priorité au sein du trafic asynchrone d'une station, ce qui permet de contrôler la bande passante offerte aux différentes sources asynchrone.

6 Interconnexion de réseaux locaux : les ponts

Nombreuses sont les entreprises qui disposent de plusieurs réseaux LAN différents, qu'elles souhaitent le plus souvent interconnecter afin de constituer leur réseau d'entreprise. Les réseaux LAN peuvent être interconnectés au moyen de divers types d'équipements, comme par exemple les ponts (*bridge*), qui interviennent fonctionnellement au niveau de la couche liaison de données.

Les ponts ont apparu sur le marché au début des années 80. Les premiers ponts interconnectaient des réseaux homogènes, c'est-à-dire du même type, comme par exemple deux réseaux Ethernet. Plus récemment, l'utilisation de ponts entre des réseaux différents à été normalisé.

Les ponts permettent donc d'interconnecter plusieurs réseaux locaux. Ou, vu d'une autre manière, les ponts permettent de séparer un réseau local en plusieurs réseaux distincts.

NB : Dans les réseaux locaux actuels, les ponts ont été largement remplacés par des commutateurs. Au niveau de l'interconnexion de LAN, les ponts et les commutateurs sont équivalents ; ils implémentent les mêmes fonctions. Dans la description suivante nous utilisons toujours le terme pont pour designer à la fois les ponts et les commutateurs.

6.1 Fonctionnement des ponts

Les ponts travaillent au niveau de la couche 2 de la hiérarchie OSI. Un pont analyse une trame entrant, décide vers quel port de sortie elle doit être acheminée et transmet la trame sur ce port. La sélection du port de sortie peut se baser sur un apprentissage dynamique de la topologie du réseau, sur une configuration statique ou sur des informations contenues dans les trames. Un pont est donc capable de filtrer le trafic. Il n'envoie une trame que le port derrière lequel se trouve le destinataire et diminue ainsi la charge des réseaux.

Un pont sert aussi à interconnecter des réseaux locaux utilisant des technologies différentes, comme par exemple Ethernet et Token Ring. Cette fonction est montrée à la Figure 43.

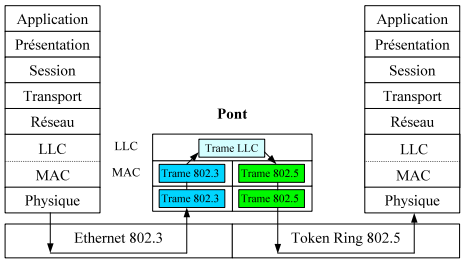


Figure 43: Interconnexion de réseaux hétérogènes à l'aide d'un pont

Le fonctionnement de ponts et de commutateurs (*switch*) et ainsi très similaire. La seule différence entre les deux équipements est qu'un pont implémente ces fonctions en logiciel, contrairement à un commutateur qui les implémente en général en matériel. Un commutateur est donc capable de travailler de travailler à une vitesse bien supérieure. C'est aussi la raison pour laquelle un commutateur à beaucoup plus de port qu'un pont, qui n'interconnecte que nombre faible de réseau. Un commutateur est donc un pont multi-port à grande vitesse.

6.2 Utilisation de ponts

Avant d'entrer dans les détails techniques des ponts, examinons quelques cas classiques d'utilisation des ponts, en commençant par mentionner les raisons principales pour lesquelles une entreprise ou une organisation se retrouve avec de multiples réseaux LAN :

Élargissement de l'étendu du réseau. Dans certains cas, un réseau LAN unique serait adéquat en terme de charge, mais la distance physique entre les machines les plus éloignées est trop importante (par exemple supérieure à 2,5 km pour les réseaux 802.3). Même si la pose du câble est facile à réaliser, le réseau ne fonctionnerait pas en raison du délai de transmission trop long. La seule solution est alors de partitionner le LAN en installant des ponts entre les divers segments du réseau.

Séparation logique. Il peut être nécessaire de diviser logiquement un réseau LAN en plusieurs segments ou LAN physiquement séparés, afin d'optimiser la charge sur le réseau. Dans un réseau comprenant un nombre important de stations, la dimension du réseau interdit de mettre toutes les stations de travail sur un réseau LAN unique - la bande passante nécessaire de ce dernier devrait être beaucoup trop importante. Au lieu de cela, on utilise plusieurs LAN interconnectés par des ponts, comme le montre la Figure 44. Chaque LAN est composé d'une grappe de stations de travail dotées de leur propre serveur de fichiers. Ainsi la majeure

partie du trafic est limitée sur le LAN local et n'ajoute pas de charge supplémentaire sur le réseau fédérateur en arrière-plan (backbone).

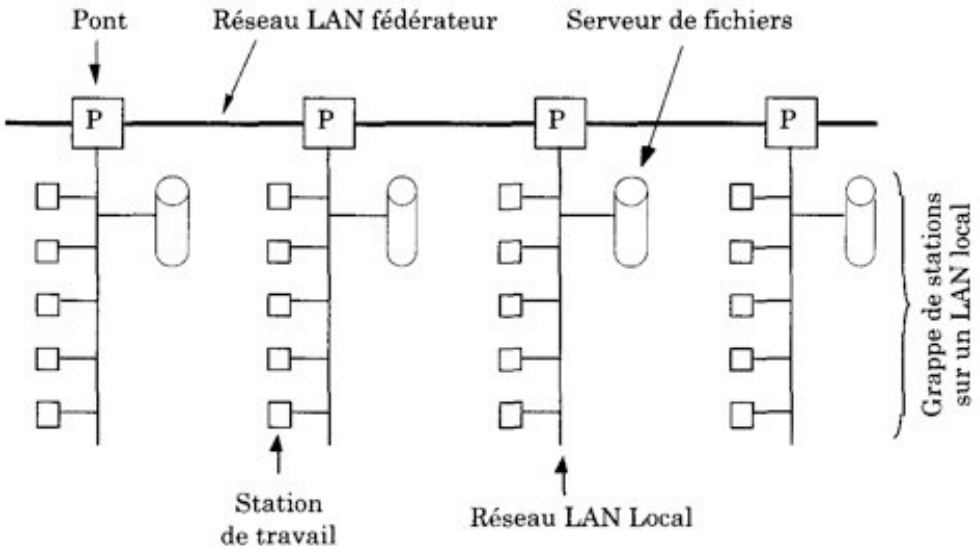


Figure 44: Séparation logique d'un réseau local à l'aide de ponts

Sécurité. Les ponts peuvent contribuer à la sécurité de la collectivité. La plupart des coupleurs de LAN peuvent fonctionner en mode transparent dans lequel toutes les trames, et non seulement celles qui lui sont adressées, sont copiées et remises à la station. Ce mode peut être exploité pour espionner des transmissions. En insérant des ponts à des endroits variés et en veillant à empêcher la transmission des éléments sensibles, il devient possible d'isoler certaines parties du réseau de façon à interdire ou filtrer l'accès aux informations qui y transitent.

Hétérogénéité des réseaux. Chaque département d'une organisation ou d'une entreprise a son propre réseau LAN, qui n'utilisent pas forcément la même technologie. Tôt ou tard le besoin d'interaction entre les départements se fait sentir, nécessitant la mise en relation des ressources informatiques; et bien évidemment l'interconnexion des réseaux LAN. C'est alors que l'usage de ponts devient nécessaire.

6.3 Types de ponts

À cause des différentes technologies utilisées dans les réseaux locaux, l'IEEE n'a pas pu aboutir à une seule norme définissant la fonctionnalité des ponts. Deux spécifications parfaitement incompatibles ont été élaborées. Les **ponts transparents** sont utilisés principalement dans les réseaux Ethernet. Les réseaux Token Ring utilisent un autre type de pont, appelé le **pont à routage par la source**. Nous allons examiner les deux types dans les sections suivantes.

L'interconnexion de réseaux Ethernet et Token Ring est loin d'être triviale. Des ponts offrant cette possibilité existe. Nous discutons les problèmes liés à cette interconnexion dans la dernière section.

6.3.1 Les ponts transparents

Le premier type de pont défini par le comité IEEE 802 est le pont transparent ou pont d'arbre recouvrant (*spanning tree bridge*). Le souci dominant de ceux qui ont soutenu ce type de pont fut la **totale transparence**. De leur point de vue, il doit suffire pour un site possédant de nombreux LAN d'aller acheter des ponts au standard IEEE, de brancher les connecteurs sur ces ponts, et tout doit fonctionner parfaitement et instantanément. Aucune modification du matériel ne doit être nécessaire, ni aucune modification du logiciel, pas non plus d'initialisation d'adresses ni de téléchargement de table de routage ou de paramètres. Il suffit seulement de brancher les câbles et de laisser faire. Le fonctionnement des LAN ne doit en aucun cas être affecté par le pont. Chose assez surprenante, cela fonctionne réellement.

6.3.1.1 Acheminement des trames

Quand une trame arrive, le pont doit décider s'il la détruit ou s'il la fait suivre, et dans ce cas, sur quel LAN il doit la faire suivre. La décision est prise en examinant l'adresse de destination de la trame afin de localiser le destinataire au moyen d'une table de localisation interne au pont. Cette table contient toutes les adresses MAC des destinations possibles. Son examen permet de dire à quelle sortie (ou à quel LAN) appartient une certaine destination.

Lorsque les ponts sont mis en place pour la première fois, toutes les tables de localisation sont vides. Ils ne connaissent aucune destination. Ils utilisent alors un algorithme d'inondation : toute trame à l'entrée d'un pont dont la destination est inconnue est envoyée sur tous les LAN raccordés au pont, excepté sur celui dont elle provient.

Au fur et à mesure que le temps passe, le pont apprend où sont situées les différentes destinations. Pour faire cela, les ponts fonctionnent en mode sans distinction et voient et enregistrent chaque trame envoyée sur chacun de leurs LAN. En examinant l'adresse source des trames ils peuvent savoir quelle machine est accessible sur quel LAN.

La topologie globale d'un réseau peut évoluer en fonction des arrêts et des remises en route des stations et des ponts; de même que leur déménagement. Périodiquement, une tâche du pont consulte les tables afin de supprimer toutes les entrées périmées. Une entrée est considérée comme périmée si elle n'a pas été mise à jour depuis un certain temps (de l'ordre de quelques minutes). De cette manière, si une station est débranchée de son LAN, déplacée dans le bâtiment puis rebranchée à un autre endroit, elle sera à nouveau opérationnelle en quelques minutes, sans intervention manuelle.

Avec cet algorithme, si une machine est silencieuse depuis quelque temps, tout trafic qui lui est destiné donnera lieu à une inondation jusqu'à sa prochaine émission de trame, qui permette sa localisation.

6.3.1.2 La topologie d'arbre recouvrant (*Spanning Tree*)

Afin d'augmenter la fiabilité, certains sites utilisent deux ponts ou plus en parallèle entre deux LAN, comme le montre la Figure 45. Cependant, cette façon de faire à tendance à créer des boucles dans la topologie du réseau et introduit ainsi quelques problèmes additionnels.

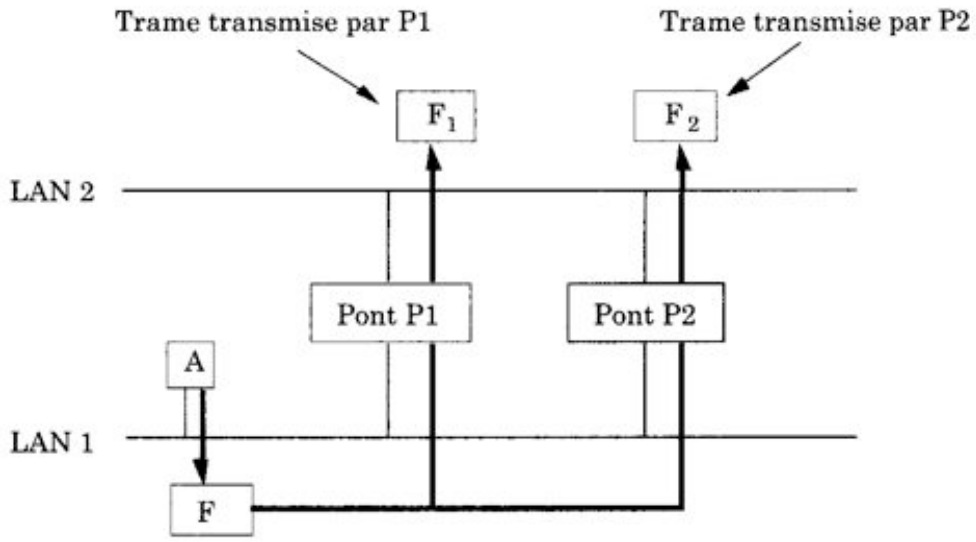


Figure 45: Deux ponts transparents parallèles

Dans une telle configuration, le mécanisme d'inondation, utilisé pour la transmission de trames avec un destinataire inconnu, peut causer un cycle infini de transmissions de la même trame.

La solution à cette difficulté consiste à faire communiquer chaque pont avec tous les autres et à superposer à la topologie réelle un **arbre recouvrant** (*spanning tree*) qui atteigne tous les LAN. Cela a pour effet **d'interdire ou d'ignorer volontairement certaines interconnexions entre LAN** dans l'intérêt de construire une topologie réseau sans boucle perturbatrice.

6.3.1.3 Construction de l'arbre recouvrant

Pour construire un arbre recouvrant sur une infrastructure de réseaux LAN interconnectés par des ponts, un algorithme automatique (et systématique) est utilisé.

1. En premier, il est nécessaire de choisir le pont qui jouera le rôle de la racine de l'arbre. Pour cela les ponts doivent se concerter et choisir. Les ponts échangent des messages appelés « Hello », dans lesquels ils indiquent leur ID (la concaténation d'une priorité configurable et l'adresse MAC du pont) ainsi que l'ID du pont qu'ils considèrent comme la racine de l'arbre. La racine est choisie comme le pont avec l'ID le plus petit. Une fois que les ponts se sont mis d'accord sur la racine, ils n'envoient plus des messages « Hello ». Seulement la racine continue à en envoyer et les autres ponts transmettent les messages sur tous les ports actifs.

2. Ensuite, chaque pont choisi son port racine. Le port racine d'un pont et celui avec la distance la plus courte vers la racine.
   Pour pouvoir déterminer la distance d'un port vers la racine, chaque port a un coût local assigné. Ce coût à une valeur par défaut qui peut être changé par l'administrateur de réseau. Les messages « Hello » émis par la racine contiennent un champ indiquant le coût du chemin traversé. Chaque pont ajoute le coût du port de réception lorsqu'il reçoit un message Hello. Puis il le

transmet sur toutes les interfaces de sortie. Ainsi, un message Hello indique toujours le coût total, c'est-à-dire la distance, vers la racine
Si le LAN contient des boucles, un pont va recevoir des messages Hello sur plusieurs ports. Il choisit le port racine comme celui sur lequel le message Hello avec le coût total minimal a été reçu.

3. Ensuite, un pont « désigné » est choisi pour chaque LAN. Le pont désigné est le pont connecté à un LAN qui offre le chemin le plus court entre ce LAN et la racine. Un port désigné doit être élu si un LAN est atteignable à travers plusieurs ponts. Lorsqu'un pont transmet un message Hello sur un port, il mémorise le coût total de ce port vers la racine. Si plus tard il reçoit sur le même port un message Hello avec un coût inférieur, il peut en déduire deux informations. Premièrement, il saura que le LAN connecté à ce port est atteignable à travers un autre pont, donc il y a une boucle dans la topologie. Deuxièmement, l'autre pont connaît un chemin plus court entre ce LAN et la racine, donc l'autre pont doit devenir le pont désigné pour ce LAN. Pour enlever la boucle, le pont met le port connecté au LAN en question dans l'état bloqué, avec l'effet qui ne va ni transmettre ni recevoir des trames sur ce port. En résumé, si un LAN est atteignable à travers plusieurs ports, un seul port reste actif. Ce port est le port désigné du LAN.

Le résultat de cet algorithme est une topologie virtuelle sans boucles. Si un pont ne reçoit pas de message « Hello » de la racine après une certaine période de temps, il recommence à en envoyer lui-même, ce qui permet d'élire une nouvelle racine en cas de panne de l'ancienne.

6.3.1.4 Changement de la topologie

Regardons maintenant comment le protocole de l'arbre recouvrant se comporte en cas de panne d'un lien ou d'un port. La Figure 46 montre une topologie LAN avec une boucle.

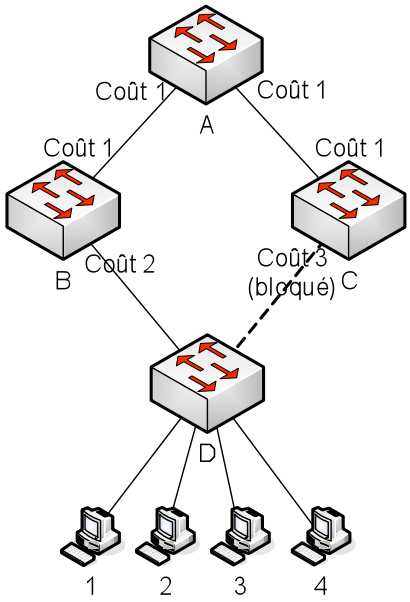


Figure 46: Topologie virtuel et coûts totaux déterminés par le protocole de l'arbre recouvrant

Les coûts totaux appris à l'aide des messages Hello sont valables pendant une durée limitée, typiquement pendant quelques dizaines de secondes. Imaginons maintenant que le lien entre les ponts B et D tombe en panne. Le pont D n'a alors plus de lien actif vers le reste du LAN. Il ne recevra plus de messages Hello de B et effacera les coûts appris pour ses ports. Il se mettre en état d'écoute et n'enverra plus de message Hello à C. Comme ce dernier ne reçoit de messages Hello que depuis A, il réactive le port vers D, qui devient alors le port désigné pour D. La nouvelle topologie virtuelle est montrée à la Figure 47.

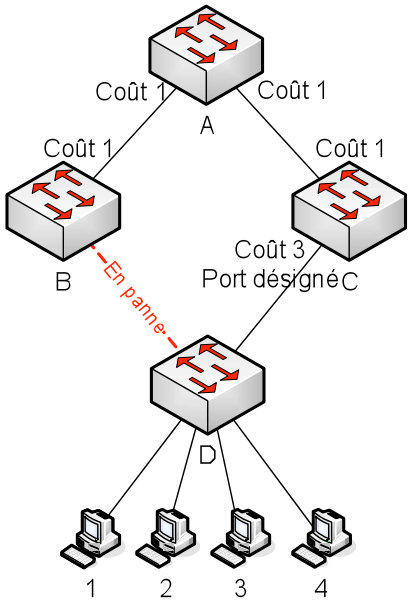


Figure 47: Topologie virtuelle après la panne du lien B-D

Or, il reste encore un problème à résoudre. Le pont A a appris (voir Sect. 6.3.1.1) que les stations 1, 2, 3 et 4 sont atteignables à travers le port vers B. Il continuera alors à transmettre des trames destinées à ces machines vers B, mais B n'est plus capable d'atteindre ces stations. Le problème sera résolu au bout de quelques minutes, quand les entrées dans la table de localisation de A ont échues. Après ce temps, A diffusera une trame destinée aux stations 1-4 sur tous les ports et apprendra – par une éventuelle réponse des machines – qu'elles sont accessibles à travers le port vers C.

Afin d'accélérer ce processus, un pont qui détecte un changement de la topologie virtuelle envoie des messages « Annonce de changement de topologie » (*Topology Change Notification*) vers la racine. Quand la racine reçoit un tel message, elle inonde le LAN avec des messages Hello qui ont un bit « Changement de topologie » positionné à 1. Tous les ponts accélèrent alors le vieillissement des informations dans la table de localisation. La durée de validité est réduite à quelques secondes au lieu de quelques minutes. Dans notre exemple, quelques secondes après la réception de l'annonce de changement de topologie, A effacera les entrées pour les stations 1-4 de sa table de localisation. Ensuite, une trame destinée à une des machines sera diffusée par A sur tous ses ports et arrivera alors au destinataire.

6.3.2 Les ponts à routage par la source (*Source Route Bridge*)

Les ponts transparents présentent l'avantage d'être faciles à installer. Il suffit de les brancher et de laisser faire. D'un autre point de vue, comme ils utilisent un sous-ensemble de liens possibles, l'utilisation de la capacité totale de transport dans le réseau n'est pas optimisée. L'importance relative de ces deux critères (entre autres) a conduit à une scission du comité IEEE 802. Les tenants de CSMA/CD et des bus à jetons ont opté pour les ponts transparents. Les tenants des anneaux, encouragés par IBM, leur ont préféré un modèle appelé routage par la source (*source routing*), que nous allons décrire maintenant.

6.3.2.1 Routage par la source

Pour l'essentiel, dans le routage par la source, celle-ci doit savoir si oui ou non le destinataire est sur son propre LAN. Lorsqu'une machine source envoie une trame sur un autre LAN, elle la marque en positionnant le bit de poids fort de l'adresse du destinataire à 1. Puis elle ajoute dans l'en-tête de la trame le chemin exact qu'elle doit suivre.

La construction du chemin est la suivante. Chaque LAN possède un numéro unique, sur 12 bits, et chaque pont possède un numéro, sur 4 bits, qui ne l'identifie que dans le contexte de son LAN. Ainsi, deux ponts éloignés peuvent chacun avoir le numéro 3, mais deux ponts sur le même LAN doivent avoir des numéros distincts. Une route est donc une suite de numéros de pont, de LAN, de pont, de LAN, etc.

Un pont utilisant le routage par la source ne va s'intéresser qu'aux trames dont le bit de poids fort de l'adresse de destination est à 1. Pour chacune de ces trames il analyse leur route en recherchant le numéro du LAN duquel elle provient. Si ce numéro de LAN est suivi par son propre numéro de pont, il transmet la trame au LAN dont le numéro suit le sien sur la route. Si le numéro de trame en entrée est suivi d'un numéro de pont différent du sien, il ne retransmet pas la trame.

6.3.2.2 Recherche des routes

Lorsqu'une station X veut envoyer des informations à une station Y, elle envoie en diffusion une **trame de découverte de chemin**. Un pont qui voit arriver une trame de ce type y ajoute sa propre adresse et retransmet cette trame vers tous les réseaux, à l'exception de celui par lequel la trame est arrivée. La station destination Y voit donc arriver une ou plusieurs trames et retourne à X toutes les trames reçues en utilisant les informations d'acheminement trouvées dans chacune. Ensuite, X peut utiliser la ou les routes que le protocole lui a permises de découvrir. Son choix est guidé par divers paramètres, tels que les délais d'acheminement, nombre de ponts traversés, … .

Bien que, de toute évidence, cet algorithme trouve la meilleure route (il les trouve toutes), il souffre d'une explosion combinatoire des trames. Considérons l'exemple de la Figure 48 ou N LAN sont interconnectés deux à deux par trois ponts. Chaque trame de recherche émise par la machine A est copiée par chacun des trois ponts du LAN 1 ; trois trames de recherche atteignent donc le LAN 2. Chacune d'elles est copiée par chaque pont du LAN 2, ce qui provoque l'arrivée de neuf trames sur le LAN 3. Lorsque le LAN N est atteint, ce sont 3^N-1 trames qui circulent. Si une douzaine d'étages de ponts sont traversés, plus d'un demi-million de trames de recherche sont injectées sur le dernier LAN, ce qui entraîne de sérieuses congestions.

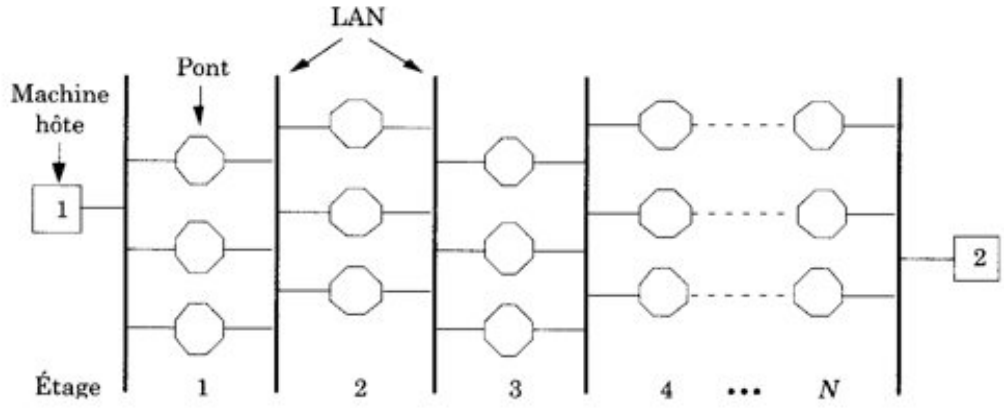


Figure 48: Une série de LAN interconnectés deux à deux par trois ponts

Une fois qu'une machine hôte a trouvé une route pour une certaine destination, elle la stocke en mémoire cache afin que le processus de recherche de route ne soit pas exécuté à nouveau la fois suivante. Si cette approche limite grandement l'impact de l'explosion des trames, il alourdit toutefois l'administration de chacune des machines hôtes du réseau et l'algorithme global n'est définitivement plus transparent, ce qui était pourtant l'un des objectifs principaux de ce type de pont.

6.4 Interconnexion de LAN hétérogènes

Comme indiqué dessus, il existe des ponts qui permettent d'interconnecter des réseaux locaux de technologies différentes. Pourtant, une telle interconnexion ne peut pas être parfaite. Dans cette section, nous montrons quelques-unes des difficultés rencontrées lorsqu'on essaie de mettre en place un pont entre divers types de LAN 802.

Débits de transmission différents. Les LAN interconnectés n'ont pas nécessairement des débits binaires identiques. Lors d'un transfert important de trames successives d'un LAN rapide vers un LAN plus lent, un pont sera incapable de délivrer les trames aussi rapidement qu'elles lui arrivent. Il devra les mémoriser, en espérant ne pas tomber à court de place mémoire.

Format de trames incompatibles. Chaque réseau LAN utilise un format de trame différent. En conséquence toute transmission entre différents LAN impose une mise au format respectif des trames, ce qui prend du temps mais ne représente pas de difficultés insurmontables.

Longueur de trames incompatibles. Le problème potentiellement le plus sérieux de tous, provient du fait que les trois LAN 802 ont une longueur maximale de trame différente. Pour le 802.3, la longueur maximale d'une trame est de 1518 octets. Pour le LAN 802.5, il n'impose pas de limite supérieure, hormis le fait qu'une station ne peut émettre plus longtemps que le temps de possession du jeton. La valeur par défaut de ce temps, de 10 ms, permet une longueur maximale de trame de 5 000 octets. Comme les ponts ne sont pas capables de fragmenter et réassembler des trames, les **trames trop longues doivent être rejetées**.

Bits de signalisation. Un autre problème provient des bits A et C du champ « Statut » de la trame Token Ring. Ces bits sont positionnés par le destinataire pour indiquer à l'émetteur si la station adressée a vu ou non la trame et si elle l'a recopiée. Ethernet n'utilise pas ces bits et en conséquence un destinataire se trouvant sur une LAN Ethernet ne pourra pas confirmer la réception de la trame. Le pont peut « mentir » et dire que la trame a été copiée, mais si plus tard il s'avère que le destinataire est hors course, des problèmes se posent. En substance, l'insertion d'un pont entre ces réseaux a modifié la sémantique des bits. Il est difficile d'imaginer une solution nette à ce problème.

En résumé, il n'y a pas de solution parfaite pour interconnecter des technologies LAN par des ponts. Une partie de la fonctionnalité des différentes technologies doit être sacrifiée. Une autre solution et l'interconnexion par des routeurs, c'est-à-dire l'interconnexion au niveau de la couche 3.

6.5 Ethernet commuté

Nous avons décrit en détail les techniques utilisées dans les réseaux Ethernet partagés, dans lesquels un média physique (le bus) est partagé par plusieurs machines. La bande passante du média doit être partagée entre toutes les stations connectées au réseau. Dans un réseau FastEthernet avec un nombre maximal de 1024 stations connectées, chaque station peut disposer d'un débit moyen de moins de 100 kb/s.

Une solution pour augmenter le débit disponible s'impose depuis le début des années 90 avec l'Ethernet commuté. La configuration d'un tel réseau prend une topologie en étoile, tant au niveau physique (câblage) qu'au niveau logique. Un commutateur (*switch*) sert de nœud central du réseau, avec les différents segments Ethernet reliés à un des ports du commutateur.

La fonction principale d'un commutateur est de diriger une trame reçue sur un de ces ports vers un ou plusieurs ports de sortie, sur lesquels la trame sera transmise. Il

travaille au niveau de la couche liaison du modèle OSI et interprète les trames reçues (Figure 49).

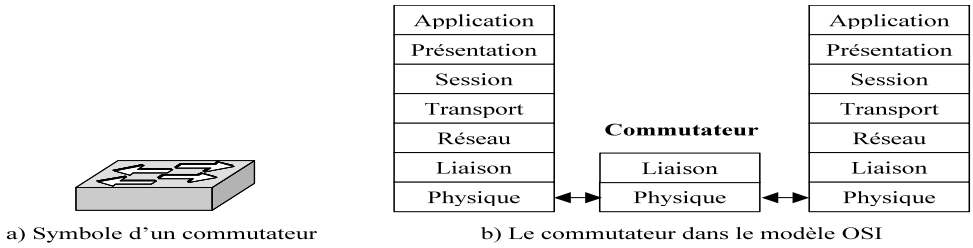


Figure 49: Commutateur

Les segments connectés au commutateur peuvent être des segments partagés (*segment based switching*) ou des liens point à point entre une station et le commutateur (*port based switching*), comme montré dans la Figure 50.

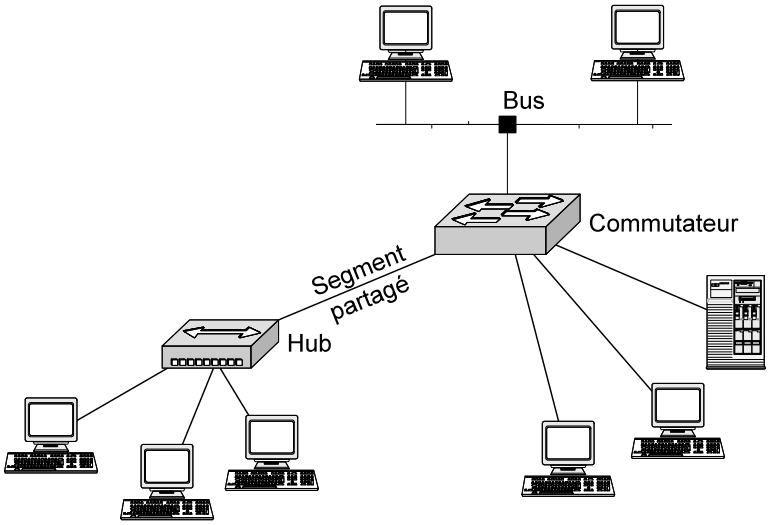


Figure 50: Ethernet commuté, interconnectant des segments point à point et partagés

6.5.1 Commutation

La structure interne d'un commutateur est montrée sur la Figure 51.

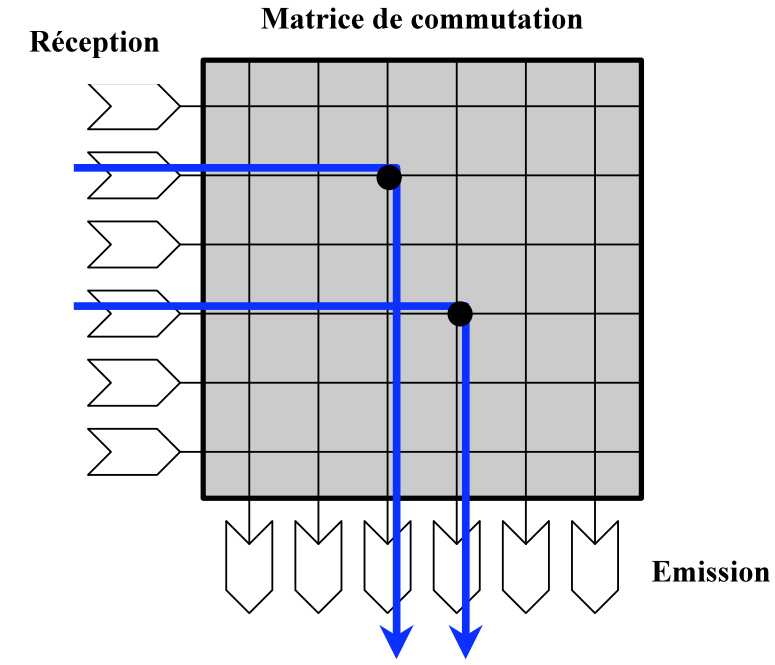


Figure 51: Structure interne d'un commutateur

Chaque port d'un commutateur est composé d'un émetteur et d'un récepteur qui sont connectés à une matrice de commutation. Cette structure en matrice n'est qu'une représentation conceptuelle. En réalité, les architectures des commutateurs peuvent être très complexes et chaque fabricant essaie d'optimiser les performances des ses commutateurs. Ce qui est important est le fait que plusieurs trames puissent être commutées en même temps par un commutateur. Les ports sont donc indépendants l'un de l'autre et il n'y a pas de collisions entre trames reçues et émises sur des ports différentes. Ceci est la différence principale par rapport à un hub, qui n'est capable que de traiter une seule trame à la fois. Un commutateur **sépare donc les domaines de collisions**. Chaque port représente un domaine de collision séparé (entre le commutateur et la ou les stations connectées sur le port). Les collisions d'un segment connecté n'affectent pas les autres segments.

Il existe plusieurs techniques de commutations.

6.5.1.1 Cut-through switching

Ce type de commutation consiste à émettre vers le destinataire aussitôt que possible sans attendre la réception de la trame entière. L'en-tête de chaque trame (au minimum les premiers 6 octets contenant l'adresse du destinataire) est directement décodée et la trame acheminée vers le port de sortie. Ceci peut se faire par des processeurs dédiés (ASIC). Ce type de switch ne nécessite pas de mémoire tampon important et assure un temps de latence constant et très court. Le temps de latence n'est cependant pas aussi court que celui d'un répéteur car il faut attendre la réception de l'entête de la trame

(préambule + l'adresse de destination + temps de commutation) ce qui équivaut à environ 140 temps de bit, c'est-à-dire 1,4 ms pour un switch travaillant à 100 Mb/s.

Les inconvénients de cette méthode sont :

- Utilisation d'un processeur dédié: solution rapide mais non évolutive.
- Pas de contrôle d'erreur: les trames sont transmises avant de pouvoir vérifier le champ FCS de la trame afin de détecter des trames erronées.
- Ne permet pas la conversion de vitesse de transmission, p. ex. entre des segments FastEthernet à 100 Mb/s et un segment d'épine dorsale Gigabit-Ethernet.

C'est la technique de commutation la plus rapide rendue publique.

6.5.1.2 Store and Forward

Chaque trame est complètement stockée avant d'être analysée. Le temps de latence dépend de la longueur des trames. Chaque trame peut être analysée et contrôlée (FCS) avant d'être commutée. Des filtrages supplémentaires peuvent être mis en place. Cette solution est implémentée par des processeurs classiques RISC ce qui permet une mise à jour du code exécuté.

Les inconvénients sont

- Temps de latence plus élevé.
- Nécessite une mémoire tampon de grande taille.

Les avantages de cette méthode :

- L'implémentation logiciel est possible, ce qui rend cette méthode plus évolutive (VLAN: réseaux virtuels, routage intégré, filtrage).
- Les trames transmises sont correctes.
- Adapté aux configurations asymétriques (permet d'interfacer des débits de 10/ 100/1000 Mb/s).

6.5.1.3 Adaptive error-free switching

Des solutions mixtes et adaptatives ont aussi été développées. Le commutateur travaille en mode *cut-through* en vérifiant l'intégrité des trames au vol. Cette vérification ne peut pas arrêter la trame, mais si plusieurs trames consécutives sont détectées en erreur, le commutateur repasse en mode *store and forward*.

6.5.2 Ethernet full-duplex

Full-duplex est un mode d'opération optionnel de cartes réseau sur des liens point à point. La transmission full-duplex est conceptuellement beaucoup plus simple que la transmission half-duplex sur un lien ou segment partagé. Aucune méthode de résolution de contention n'est nécessaire, il n'y a pas de collisions et les méthodes de retransmission sont superflues. En effet, la méthode CSMA/CD n'est plus utilisé. Ceci résulte en plus de temps disponible pour la transmission mais aussi en un

redoublement de la bande passante d'un lien en permettant deux transmissions simultanées au débit nominal du lien.

La transmission peut être initiée aussitôt qu'une trame est prête pour l'émission. La seule restriction est que l'interframe gap entre deux trames successives, défini dans la norme 802.3, doit être respecté.

Une conséquence importante de l'opération full-duplex est que **la longueur d'un segment n'est plus limitée** à cause du délai maximum aller-retour, comme il n'y a plus de collision. On peut réaliser des réseaux à la taille de la planète, en utilisant des répéteurs pour compenser l'affaiblissement du signal sur le support physique.

6.5.3 Filtrage de trames

Un commutateur doit déterminer le ou les ports de sortie sur lesquels il doit acheminer une trame reçue. Le port sur lequel une station avec une adresse MAC donnée peut être atteinte n'est pas pré-configuré. Au contraire, le commutateur apprend cette relation pendant l'opération. Lors de la réception d'une trame il examine l'adresse MAC de la source et mémorise le port sur lequel cette station est atteignable. Pour déterminer le port vers lequel une trame reçue doit être acheminée, il examine l'adresse MAC du destinataire de la trame et cherche le port correspondant. Ainsi, le commutateur filtre le trafic qui est envoyé vers chaque segment connecté, contrairement à un hub. Si le commutateur ne connaît pas le port sur lequel se trouve un destinataire, il revient au comportement d'un hub et diffuse la trame sur tous les ports sauf celui de réception de la trame.

6.5.4 Contrôle de flux

Bien que le mode commuté offre beaucoup d'avantages dans un réseau Ethernet, il y a aussi des inconvénients. Le premier concerne la gestion de congestions éventuelles au sein d'un commutateur. Un commutateur peut subir une congestion si les trames arrivent plus vite que le commutateur ne peut les écouler, p. ex. dans une configuration asymétrique (10/100 Mb/s) ou parce que beaucoup de trames reçues doivent être commutées vers le même port de sortie. Pour résoudre ce problème il faut mettre en place un contrôle de flux qui permette un commutateur détectant une congestion de demander l'arrêt de transmission à un nœud émetteur.

Ce contrôle est réalisé au niveau de la couche MAC et utilise des trames « Pause » qui envoyées par le récepteur à un nœud émetteur. C'est un contrôle de type back-pressure, dans lequel l'information de congestion remonte jusqu'à la source, nœud par nœud. Le nœud amont est informé d'une demande d'arrêt des émissions, avec précision du temps pendant lequel il doit rester silencieux. Cette période peut être brève, si le nœud est peu congestionné, ou longue, si le problème est important. Le nœud amont peut lui-même estimer, suivant la longueur de la période de pause imposée, s'il doit faire remonter un signal Pause ou non vers son nœud amont (Figure 52).

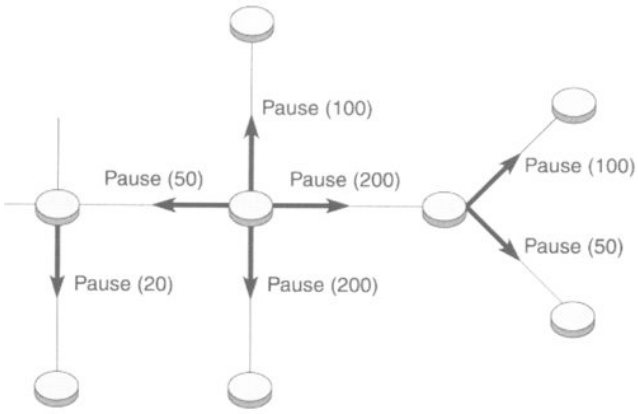


Figure 52: Contrôle de flux dans un réseau Ethernet commuté

6.5.5 Gestion d'adresses

Un deuxième inconvénient de la commutation Ethernet est la nécessité de gérer les adresses de nœuds atteignables à travers un port. Dans un réseau important, cette information peut consommer une quantité de non-négligeable de la mémoire d'un commutateur. Cette information doit être consultée pour chaque trame reçue afin de déterminer le port de sortie. Naturellement, la recherche dure d'autant plus long que la liste d'adresses est grande. La seule solution à ce problème est la limitation du nombre d'adresse qu'un commutateur doit mémoriser. Nous allons voir plus loin comment la technique des VLAN (*virtual LAN*) permet de résoudre ce problème.

6.6 Réseaux locaux virtuels (VLAN)

Nous avons vu que l'interconnexion de réseaux locaux à l'aide de ponts et de commutateurs crée un grand domaine administratif avec les caractéristiques suivantes :

- Les ponts et commutateurs doivent connaître la localisation de chaque station connectée au domaine afin de décider sur quel port une trame doit être commutée. Dans un domaine très grand, la gestion de ces informations peut surcharger les commutateurs et pont.
- Des trames de diffusion se propagent dans le domaine entier. En conséquence, on parle d'un **domaine de broadcast**. Cette diffusion de trames à travers le domaine entier peut fortement augmenter le trafic dans le réseau, surcharger les stations terminales et poser des problèmes de sécurité.

La solution à ces deux problèmes et la configuration de réseaux locaux virtuels (VLAN). Un VLAN est un ensemble logique de stations dans un réseau local. Les réseaux VLAN résolvent ces problèmes en divisant un LAN en plusieurs domaines plus petits, chacun représentant un LAN virtuel.

Les VLAN offrent les fonctionnalités suivantes :

- **Contrôle des diffusions générales**. A l'instar des commutateurs qui isolent les domaines de collision pour les hôtes connectés et ne transmettent que le trafic approprié sur un port approprié, les VLAN implémentent entre eux une

isolation complète et affinent d'avantage ce concept de segmentation. Les trames de diffusion reste à l'intérieur du VLAN d'origine et ne peuvent pas affecter les autres VLAN.

- **Sécurité**. Les VLAN apportent la sécurité sous deux formes :
    - Les utilisateur à forts privilèges peuvent être groupés dans un VLAN, si possible sur le même segment physique, et aucun utilisateur en dehors de ce VLAN ne peut communiquer avec eux.
    - Comme les VLAN sont des groupes logiques qui se comportent comme des entités physiques séparées, la communication inter-VLAN est réalisée au moyen d'un routeur. Lorsqu'elle a lieu, toutes les fonctions de sécurité et de filtrage assurées traditionnellement par les routeurs, comme par exemple par un firewall, peuvent être utilisées.
- **Administration de réseau**. Le groupement logique des utilisateurs, sans relation avec leur situation physique ou géographique, facilitée l'administration du réseau. Il n'est plus nécessaire de tirer des câbles pour déplacer un utilisateur d'un réseau à un autre. Les ajouts, les déplacements et les changements sont réalisés en assignant le port auquel un utilisateur est connecté au VLAN souhaité.

Le VLAN introduit donc une notion de segmentation de grands réseaux, les utilisateurs étant regroupés suivant des critères à déterminer. Un VLAN peut être défini comme un domaine de broadcast dans lequel l'adresse de diffusion atteint toutes les stations appartenant au VLAN. La Figure 53 montre ce principe.

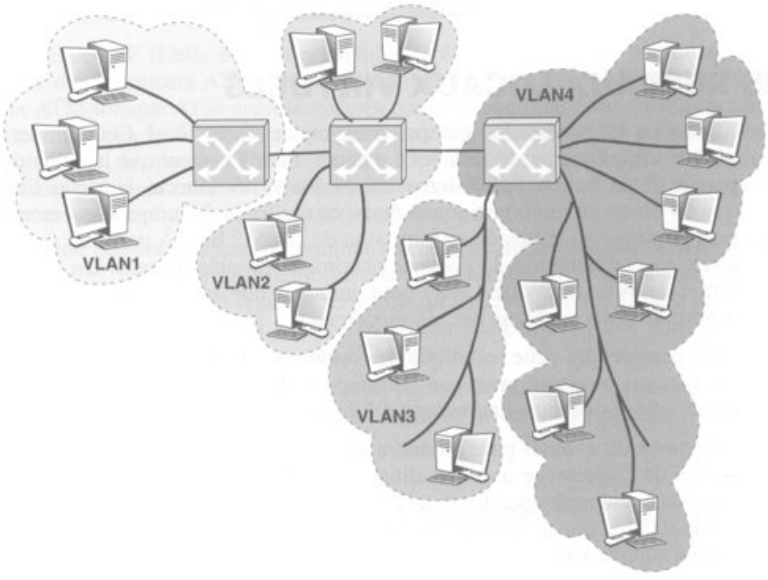


Figure 53: Séparation d'un réseau local en plusieurs VLAN

6.6.1 Implémentation de VLAN

Plusieurs types de VLAN sont possibles suivant le critère de regroupement des stations du système.

Le VLAN par port. Chaque port d'un switch est assigné à un VLAN et toutes les stations connectées sur un port font automatiquement partie de ce VLAN. C'est la méthode de définition de VLAN la plus simple. Les stations appartenant au même VLAN peuvent échangé des trames à travers le switch et font partie du même domaine de broadcast. Le trafic entre VLAN différents doit être routé. La Figure 53 montre des VLAN par port.

Le VLAN par adresse IP. Les VLAN basés sur les adresses IP définissent un VLAN à l'aide d'une liste d'adresses IP qui font partie du VLAN. La Figure 54 montre une configuration VLAN basée sur des adresses IP. Le VLAN1 comprend toutes les machines du sous-réseau 198.78.55.0/24, le VLAN2 toutes la machines du sous-réseau 198.78.42.0/24. Cette méthode permet à un seul port de commutateur de supporter plus d'un VLAN. L'avantage est qu'une machine peut être déplacée sans qu'une modification de la configuration soit nécessaire. L'inconvénient de cette méthode est que le switch doit inspecter les en-têtes IP des paquets.

Le VLAN par valeur définie par l'utilisateur. Ce type de VLAN est le plus flexible et sa définition se fonde sur la valeur de n'importe quel champ d'un paquet. Par exemple, on pourrait définir des VLAN séparés en fonction du protocole de la couche 3. Ainsi on aurait des VLAN différents pour les paquets IPv4, IPv6, … La forme la plus simple de ce type de VLAN est le groupement d'utilisateurs selon leurs adresses MAC (VLAN du niveau 2).

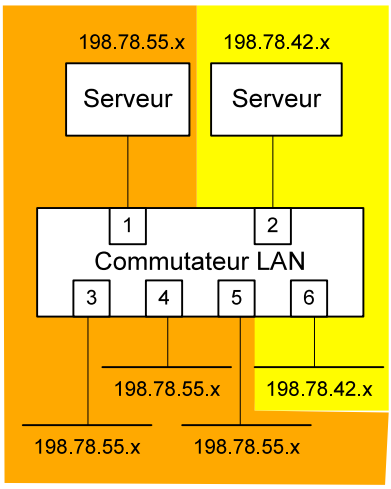


Figure 54: VLAN bases sur des adresses IP

La plupart des LAN implémente des VLAN par port. Cette méthode est la plus simple mais aussi la moins souple. Le déplacement d'une machine d'un port à un autre nécessite généralement une modification de la configuration du switch.

6.6.2 VLAN étendus

Dans un réseau impliquant plusieurs commutateurs interconnectés, la difficulté consiste à réaliser l'échange des trames à l'intérieur du VLAN même si celui-ci comprend des ports de commutateurs différents. Ceci est montré à la Figure 55.

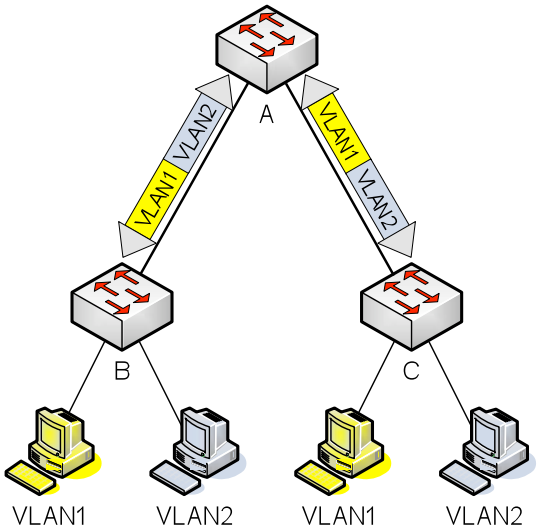


Figure 55: VLAN étendus

Dans ce scénario, les ports des switches B et C sont assignés soit au VLAN1 soit au VLAN2. Pour que toutes les machines de chaque VLAN puissent communiquer, les trames doivent passer par le switch A. Les liens entre A et B et entre A et C doivent alors transporter les trames des deux VLAN. On appelle ces liens « tronçons VLAN » (*VLAN trunks*). Pour s'assurer qu'une trame en provenance du VLAN1 sur la switch B à destination d'une machine connectée au switch C reste à l'intérieur du VLAN1, l'information concernant le VLAN d'origine doit être ajoutée à la trame lorsqu'elle est envoyée sur un tronçon VLAN. Le switch B qui reçoit une trame la classifie en déterminant à quel VLAN elle appartient, selon les critères mentionnés ci-dessus. L'identificateur du VLAN est alors ajouté dans la structure de la trame Ethernet. Quand le switch C reçoit la trame, il extrait l'identificateur du VLAN et ne transmet la trame que sur un port qui fait partie de ce VLAN.

Deux méthodes différents sont utilisées en pratique pour réaliser des VLAN étendus :

- La norme 802.1Q, appelée *VLAN tagging*, qui est une norme officielle.
- Le protocole ISL (Inter-Switch Link) qui est un protocole propriétaire Cisco mais très répandu en pratique.

6.6.2.1 VLAN tagging

La norme 802.1Q définit une extension du format de la trame Ethernet. Le format d'une trame utilisant l'encapsulation 802.1Q est montré à la Figure 56.

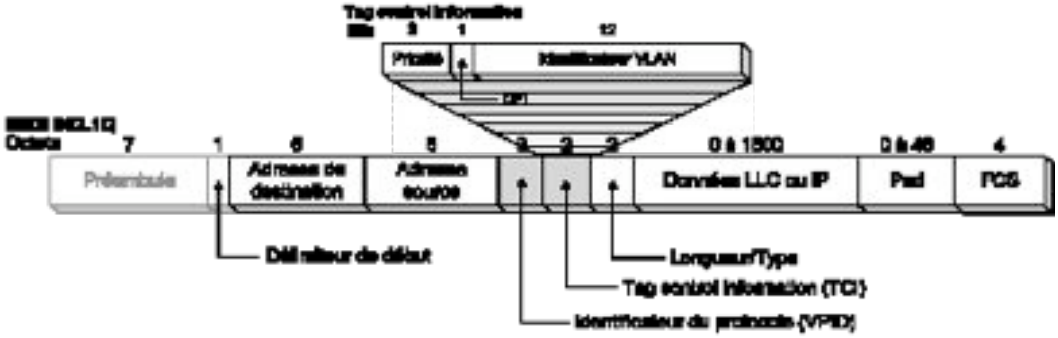


Figure 56: Format de trame selon IEEE 802.1Q (VLAN tagging)

Les 4 octets supplémentaires contiennent un premier champ VPID (VLAN Protocol IDentifier) et un champ TCI (Tag Control Information). Le VLAN tag est inséré entre l'adresse source et le champ Longueur/Type de la trame MAC. La longueur maximum de la trame Ethernet, à l'origine 1518 octets, passe alors à 1522 octets avec ce champ.

Le champ VPID a la valeur Ox8100 hex lorsque le champ TCI est présent. Le champ TCI contient principalement un champ VID (VLAN IDentifier) de 12 bits, qui indique le VLAN auquel la trame appartient. Ainsi, l'identificateur VLAN permet de distinguer au maximum 4096 VLAN différents dans un seul LAN.

Les ports d'un commutateur sont généralement configurés de manière qu'ils ajoutent et enlèvent le VLAN tag d'une trame. Ainsi, cette information n'est utilisée que pour la signalisation entre les commutateurs, donc sur les tronçons VLAN, sans que les stations terminales doivent implémenter la norme 802.1Q.

Sur chaque switch, l'administrateur de réseau doit configurer les ports qui servent de tronçons, afin de les autoriser à transmettre des trames de plusieurs VLAN. Souvent les commutateurs permettent de définir l'ensemble des VLAN autorisés séparément pour chaque port tronçon.

6.6.3 Inter-Switch Link

ISL (Inter-Switch Link) est une méthode propriétaire de Cisco pour l'encapsulation de trames LAN dans un en-tête supplémentaire qui permet de transporter entre autres l'identificateur VLAN d'une trame. Cette encapsulation n'est utilisée qu'entre les switch Cisco. Les équipements d'autres constructeurs ou les stations terminales ne comprennent pas ce format. A l'origine, ISL était supérieur à 802.1Q comme il permet l'établissement d'un arbre recouvrant par VLAN, contrairement à 802.1Q qui utilise la même topologie virtuelle pour tous les VLAN. Entre-temps, Cisco a introduit le protocole propriétaire PVST+, qui permet de établir une topologie virtuelle par VLAN même lorsque l'encapsulation 802.1Q est utilisée. Pour cette raison, Cisco recommande l'utilisation de 802.1Q si les commutateurs le permettent.

Le format d'une trame ISL est montré à la Figure 57. Comme ce format n'est pas spécifique à Ethernet, la trame encapsulée peut avoir une taille maximum de plus de 24000 octets.

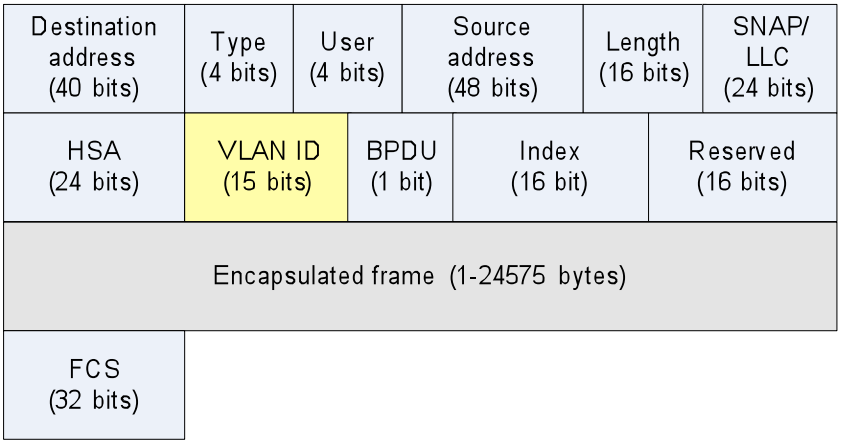


Figure 57: Format de trame ISL

Dans un contexte VLAN seul le champ VLAN ID est intéressant. Il code l'identificateur VLAN sur 15 bit. Bien que ceci permettrait de distinguer 32768 VLAN, les switches Cisco typiquement ne permettent qu'un maximum de 1000 VLAN.

6.6.4 Protocoles de gestion de VLAN

Afin de faciliter la gestion de réseaux locaux avec un nombre important de VLAN, Cisco a développé plusieurs protocoles propriétaires.

Le protocole **DTP** (*Dynamic Trunking Protocol*) peut être utilisé par des switch voisinés afin de négocier si le lien entre les switches doit être un tronçon VLAN et le cas échéant, quel format d'encapsulation VLAN est utilisé. Pour chaque port l'administrateur peut définir les options de trunking comme auto, on, off, desirable ou non-negociate qui déterminent si le port va essayer de négocier le VLAN trunking avec son pair. Typiquement, tous les ports sauf les ports d'accès (connectés aux stations terminales) deviennent automatiquement des tronçons VLAN.

Le protocole VTP (VLAN Trunking Protocol) facilite la gestion de VLAN dans un LAN important. Il permet d'ajouter, effacer et modifier des VLAN sur un switch (serveur VTP). Grace à VTP, cette information est communiquée à tous les autres switches (clients VTP) d'un domaine de gestion. Ainsi la cohérence de la configuration de tous les switches est assurée.

6.6.5 Spanning Tree et VLAN

A l'origine, l'encapsulation avec 802.1Q ne permettait qu'une seule topologie virtuelle (spanning tree) commune entre tous les VLAN. Or, dans la pratique il se pose souvent le problème de repartir le trafic sur plusieurs tronçons VLAN, comme montré à la Figure 58.

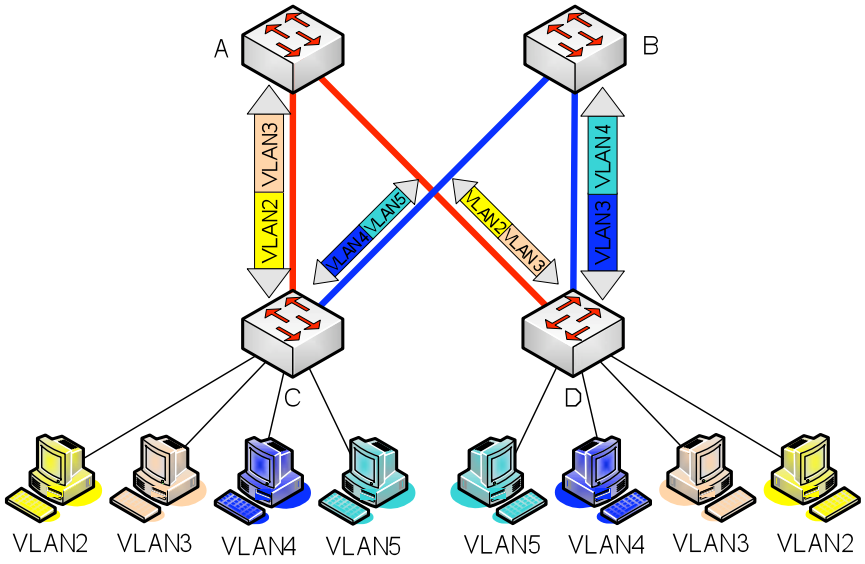


Figure 58: Répartition du trafic sur plusieurs tronçon VLAN à l'aide de plusieurs Spanning Tree

Le résultat du protocole Spanning Tree normal dans une telle topologie est montré à la Figure 59.

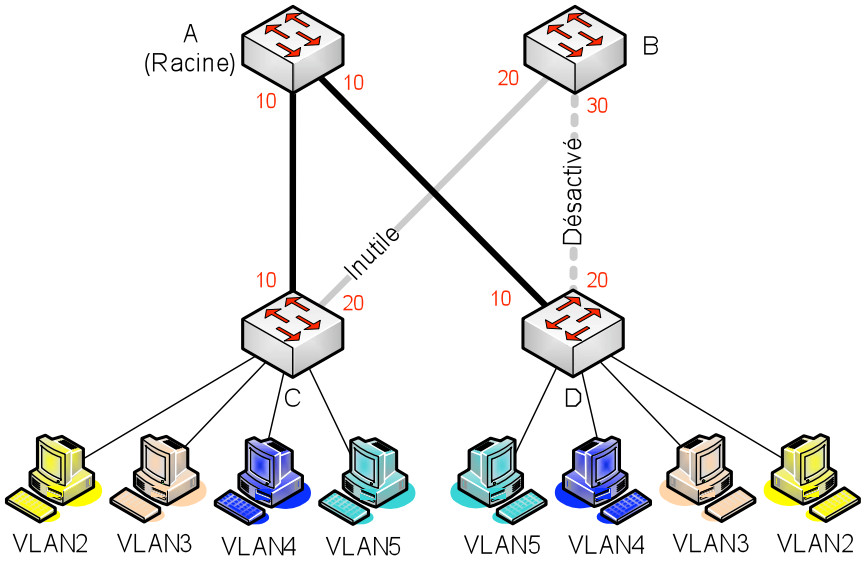


Figure 59: Topologie virtuelle avec un seul Spanning Tree pour tous les VLAN

Afin de résoudre ce problème, l'IEEE a défini le protocole 802.1s (*Multiple Spanning Tree Protocol*, MSTP) qui est une amélioration des protocoles propriétaires PVST (*Per-VLAN Spanning Tree*) et MISTP (*Multiple Instances Spanning Tree Protocol*) de Cisco. MSTP permet de créer plusieurs instances de Spanning Tree (MSTi, MST Instance) et d'associer chaque VLAN à une des instances. Pour chaque MSTi, la priorité de racine et les coûts de port (pour calculer le coût du chemin vers la racine) peuvent être configurés séparément sur chaque switch. Ensuite, chaque instance de Spanning Tree effectue l'algorithme Spanning Tree habituel, en tenant compte uniquement des paramètres de configuration associés à l'instance.

En résultats, différentes instances peuvent avoir des racines différentes, ou partager la même racine. Un port d'un switch peut être actif pour une instance et bloqué pour un autre.

Dans notre exemple, une MSTi 2 peut être configurée pour les VLAN 2 et 3 et une MSTi 3 pour les VLAN 4 et 5. Les priorités de racine des switches A et B sont à configurer de la manière suivante :

- Switch A :
  - Priorité racine MSTi 2 : 8192
  - Priorité racine MSTi 3 : 32768
- Switch B :
  - Priorité racine MSTi 2 : 32768
  - Priorité racine MSTi 3 : 8192

Le résultat de cette configuration est montrée à la Figure 60.

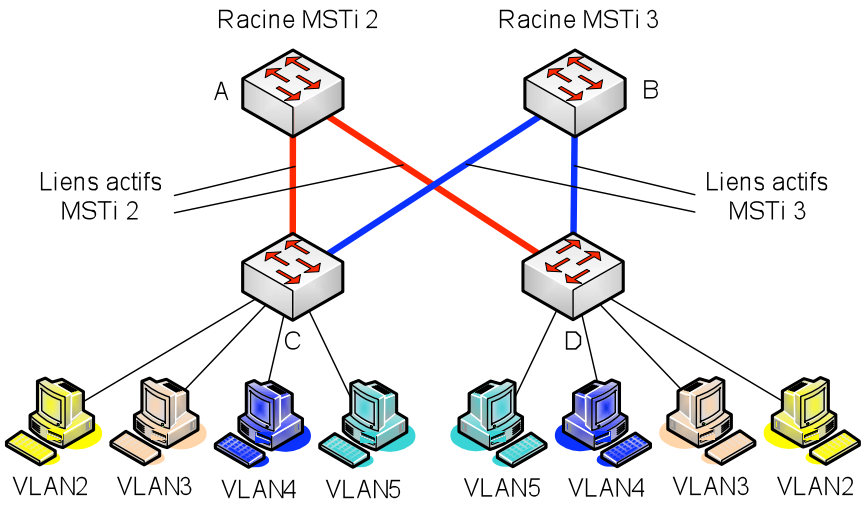


Figure 60: LAN avec plusieurs instances de Spanning Tree

6.6.6 Routage entre VLAN distincts

Le but des VLAN étant une segmentation logique d'un réseau local en plusieurs domaines distinct, il est clair que la communication entre VLAN distincts nécessite des mécanismes supplémentaires. En effet, le passage d'un VLAN à un autre se fait par l'intermédiaire d'un routeur, donc au niveau 3. Deux configurations de routage entre VLAN sont courantes.

La première configuration, montrée à la Figure 61 est utilisable lorsque le LAN ne comprend que très peu de VLAN.

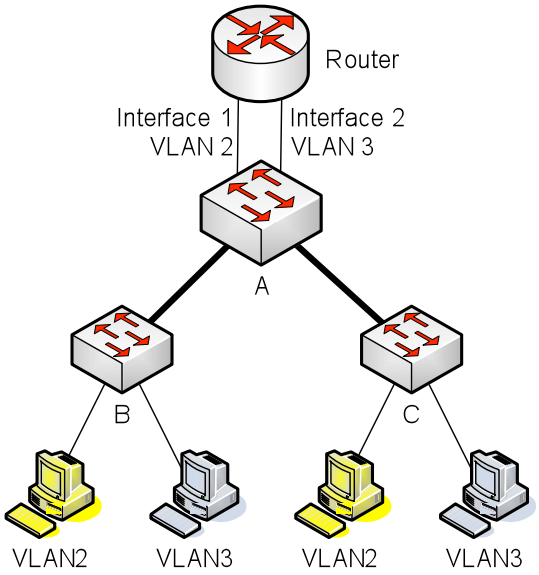


Figure 61: Routage entre VLAN avec une interface routeur par VLAN. Le VLAN tagging est effectué par le switch A.

Dans cette configuration, le routeur utilise une interface par VLAN. Chaque interface du routeur est connecté sur un port switch du type « Accès », donc attribué à un seul VLAN. En conséquence, chaque interface du routeur fait partie d'un autre VLAN. Les trames reçues depuis le switch utilisent le format Ethernet normal, sans encapsulation VLAN et ne port donc aucune information concernant l'appartenance à un VLAN. Dans cette configuration, les VLAN sont donc complètement transparents pour le routeur. Il prend les décisions de routage en fonction des adresses IP, et envoie les trames sur l'interface idoine. Chaque VLAN doit alors correspondre à un sous-réseau IP différent. Nous allons étudier la notion de sous-réseau IP dans le Chapitre 3 de ce cours. Comme une trame envoyée par le routeur est reçue par le switch sur un port d'accès, c'est le switch qui marque la trame avec le VLAN associé au port, si nécessaire.

L'avantage de cette configuration est que le routeur ne doit pas gérer les différents VLAN. En effet, un routeur sans la fonctionnalité VLAN est utilisable dans cette configuration. L'inconvénient est que plusieurs interfaces sont nécessaires sur le routeur. Cette configuration n'est donc envisageable que pour un nombre très modeste de VLAN.

Afin de permettre l'interconnexion de beaucoup de VLAN, la plupart de routeurs implémentent la possibilité de créer plusieurs interfaces virtuelles ou sous-interfaces sur une interface physique. La configuration résultante est montrée à la Figure 62.

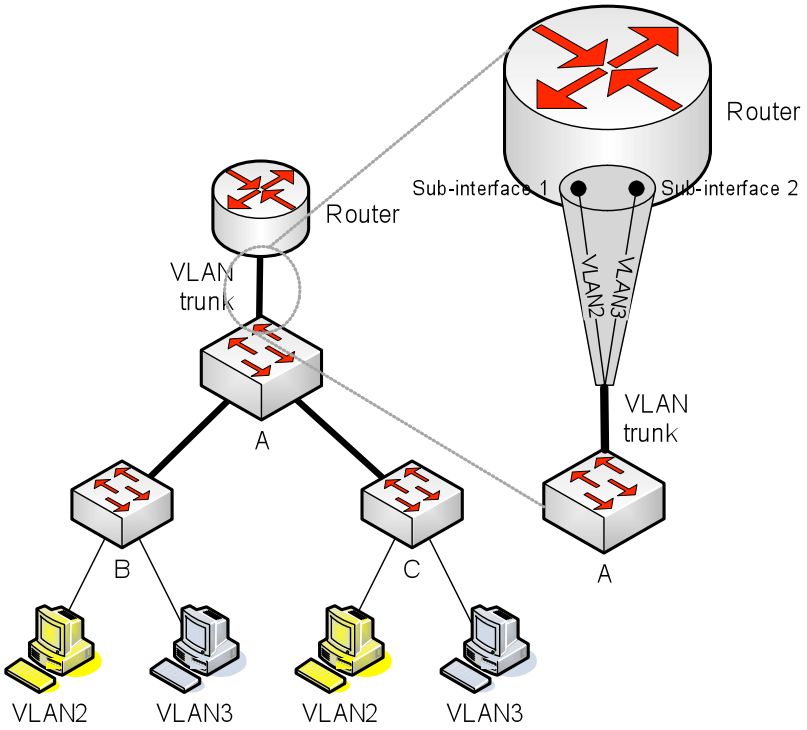


Figure 62: Routage entre VLAN avec des interfaces virtuelles sur le routeur. Le VLAN tagging est effectué par le routeur

L'interface du routeur est connectée à un port du switch qui est configuré comme tronçon VLAN. Les trames de tous les VLAN sont alors transmises sur ce lien, avec l'encapsulation VLAN. Le routeur n'utilise pas l'information sur le VLAN d'origine d'une trame pour prendre la décision du routage. Comme toujours, il ne se base que sur les adresses IP du destinataire. Cette configuration nécessite donc également que les différents VLAN fassent partie de sous-réseaux IP différents. Lorsque le routeur reçoit une trame, il enlève donc tout simplement l'encapsulation VLAN et utilise l'algorithme de routage standard.

En différence par rapport au routage normal, les interface de sortie indiqué dans la table de routage ne sont pas des interfaces physiques mais *des interfaces virtuelles*, une par VLAN. Chaque interface virtuelle est associée à un seul VLAN. Le routeur envoie alors la trame sur une interface virtuelle de sortie. L'unique but d'une interface virtuelle est de marquer une trame sortante avec le VLAN correcte, afin de l'envoyer sur un port trunk du switch connecté.

7 Les réseaux locaux sans fil

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer de place dans l'entreprise tout en restant connecté. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base. Les communications entre bornes s'effectuent de façon hertzienne ou par câbles. Ces réseaux atteignent des débits de plusieurs mégabits par seconde, voire de plusieurs dizaines de mégabits par seconde.

Plusieurs gammes de produits sont actuellement commercialisées, mais la normalisation relativement récente pourrait encore modifier les choses. Les groupes de travail qui se chargent de cette normalisation sont IEEE 802.11 aux États-Unis et HiperLAN (*High Performance Radio LAN*) sur le Vieux Continent.

- Pour les réseaux Wi-Fi, qui proviennent de la normalisation **IEEE 802.11**, les fréquences utilisées se placent dans la bande 2,4–2,483 GHz. La bande 5,15–5,3 GHz est préférée dans les nouvelles extensions.
- Pour **HiperLAN**, les bandes de fréquences retenues se situent entre 5,15 et 5,3 GHz, auxquelles il faut ajouter une bande de 200 MHz dans les fréquences autour de 17 GHz. Les vitesses de transfert, qui atteignent une cinquantaine de mégabits par seconde, pourraient concurrencer le marché des réseaux locaux filaires les plus rapides du marché. La distance entre postes de travail et stations de base peut atteindre de quelques dizaines de mètres à une centaine de mètres.

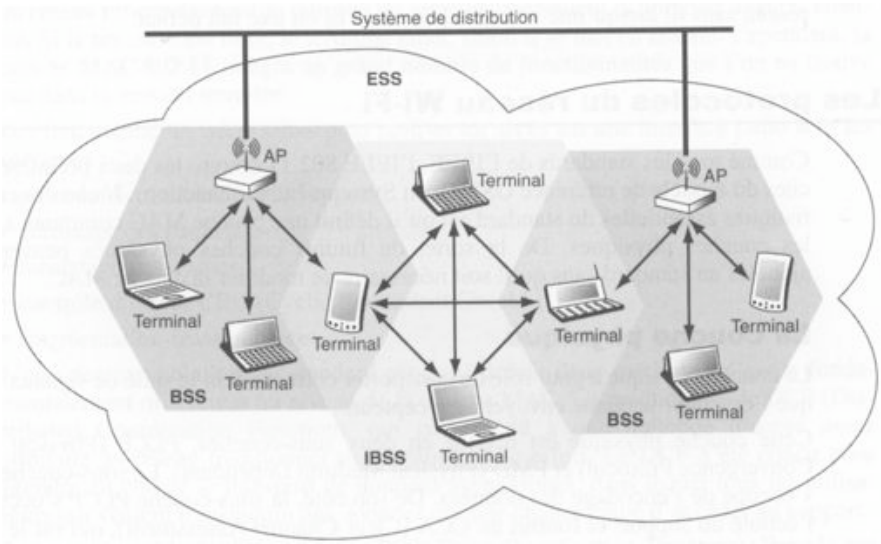
Pour la conception de systèmes WLAN, les considérations suivantes ont été tenues en compte :

1. une utilisation faible de puissance (plus longue durée des batteries),
2. technologie robuste de transmission (en vue de la mauvaise qualité du canal),
3. la possibilité d'utiliser la technologie globalement
4. transparence dans les applications (les applications existantes, conçues pour les réseaux fixes, doivent fonctionner directement),
5. une sécurité acceptable (possibilité de crypter les données transmises.)

En raison des phénomènes d'interférence dans l'interface aérienne tels que réflexions multiples, stations cachées, etc., la qualité de la transmission au niveau physique pour les systèmes sans fils est considérablement inférieure à celle d'une communication par câble torsadé, coaxial ou optique. Des taux d'erreurs de BER=10^{-4} (comparés à 10^{-10} pour les fibres optiques) sont typiques. Ce problème est exacerbé dans le cas de 802.11, 802.11b et 802.11g par le fait que de plus en plus de systèmes, tels que Bluetooth, téléphones sans fil, etc., utilisent les ondes radio dans la même plage de fréquences.

7.1 Structure des réseaux WLAN

L'architecture d'un réseau WLAN est cellulaire. Comme illustré à la Figure 63, les réseaux WLAN offrent deux modes de fonctionnement, le mode **infrastructure** et le mode **ad-hoc**.



AP (Access Point) : point d'accès
BSS (Basic Service Set) : cellule de base
ESS (Extended Service Set) : ensemble des cellules de base
IBSS (Independent Basic Service Set) : cellule de base en mode ad-hoc

Figure 63: Structure d'un réseau WLAN

Mode infrastructure

Le mode infrastructure est défini pour fournir aux différentes stations des services spécifiques, sur une zone de couverture déterminée par la taille du réseau. Les réseaux d'infrastructure sont établis en utilisant des points d'accès, ou AP (*Access Point*), qui jouent le rôle de station de base pour une BSS.

La taille des BSSs est limitée par les propriétés de propagation du milieu de transmission. Afin d'étendre la zone de couverture du réseau, plusieurs BSSs peuvent faire partie d'un réseau étendu connu comme *Extended Service Set* (ESS). Lorsque le réseau est composé de plusieurs BSS, chacun d'eux est relié à un système de distribution, ou DS (*Distribution System*), par l'intermédiaire de leur point d'accès respectif. Un système de distribution correspond en règle générale à un réseau Ethernet utilisant du câble métallique.

Deux stations dans un même BSS doivent impérativement, pour communiquer entre elles, envoyer leurs trames à leur point d'accès qui, lui, va faire la fonction de relais en transmettant la trame à la station destinataire.

La communication entre BSSs dans un ESS se fait à travers le DS. Toutes les communications de ou vers une station dans un ESS passent par un ou plusieurs points d'accès. Si les stations qui désirent communiquer se trouvent dans deux BSSs différents, la trame est adressée par la station source à son point d'accès qui, à son

tour, l'achemine par le système de distribution vers le point d'accès appartenant au BSS de la station destinataire. C'est ce dernier point d'accès qui envoie la trame à la station destinataire finale.

Mode ad-hoc

Un réseau en **mode ad-hoc** est un groupe de terminaux formant un IBSS (*Independent Basic Set Service*), dont le rôle consiste à permettre aux stations de communiquer sans l'aide d'une quelconque infrastructure, telle qu'un point d'accès ou une connexion au système de distribution. Chaque station peut établir une communication avec n'importe quelle autre station dans l'IBSS, sans être obligée de passer par un point d'accès. Comme il n'y a pas de point d'accès, les stations n'intègrent qu'un certain nombre de fonctionnalités, telles les trames utilisées pour la synchronisation.

Ce mode de fonctionnement se révèle très utile pour mettre en place facilement un réseau sans fil lorsqu'une infrastructure sans fil ou fixe fait défaut.

7.2 Les normes 802.11

Comme indiqué ci-dessus, les normes 802.11 ont été développées par l'IEEE pour le marché aux États-Unis. En Europe, les allocations des fréquences radio étant différentes, seulement la norme 802.11b est autorisée dans la plupart des pays. Cependant, les différents pays ont commencé la démarche pour libérer les bandes de fréquences concernées. La Table 14 résume les caractéristiques principales des normes.

Table 14: Caractéristiques principales des normes IEEE 802.11

Norme	Débit nominal	Commentaire	Bande de fréquences
802.11	1 et 2 Mb/s	Première norme	2.4 GHz
802.11a	54 Mb/s	Incompatible avec les autres normes 802.11b/g	5 GHz
802.11b	1, 2, 5.5, 11 Mb/s	Le plus populaire	2.4 GHz
802.11g	54 Mb/s	Compatible avec 802.11b	2.4 GHz

Les réseaux sans fils spécifiés par l'IEEE sont appelés de différentes manières : Wireless Ethernet, Wireless LAN, WLAN, Wi-Fi et 802.11x.

Il existe un programme de certification de produits 802.11x mené par la *Wireless Ethernet Compatibility Alliance* (*WECA*). Si un appareil réussi des tests de compatibilité avec les normes 802.11 ou 802.11b de la *WECA*, le fabricant a le droit d'afficher une étiquette Wi-Fi (*Wireless Fidelity*) sur le produit. Pour les produits 802.11a, l'étiquette devient Wi-Fi 5, où le 5 signifie que la fréquence radio utilisée est dans la bande de 5 GHz.

Pour les réseaux sans fil, comme pour les réseaux locaux câblés 802.3, 802.4 et 802.5, seulement la couche physique et une partie de la couche de liaisons de données sont spécifiées. La Figure 64 illustre la relation entre le modèle OSI et l'architecture définie pour les réseaux sans fil 802.11x. La couche 802.2 LLC (*Logical Link Control*) n'est pas exclusive aux réseaux 802.11 mais elle est commune à tous les réseaux locaux de la famille 802.

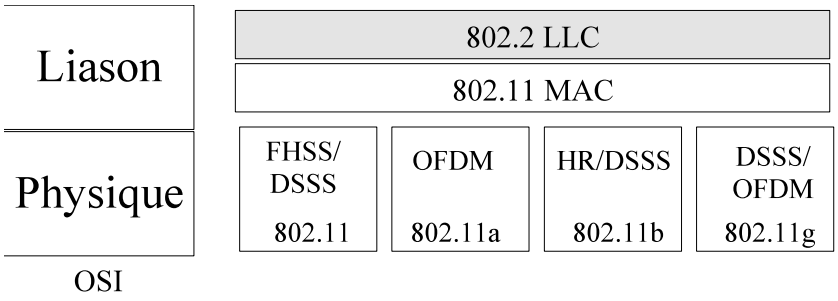


Figure 64: Les normes 802.11 dans la hiérarchie OSI

Notez qu'une seule et unique couche MAC est définie. Par contre, cinq couches physiques sont spécifiées (une des couches, basée sur l'infrarouge n'est pas représentée).

Comme illustré dans la Figure 65, la couche physique de 802.11x est divisée en deux sous couches :

- PMD (*Physical Medium Dependent*) et
- PLCP (*Physical Layer Convergence Procedure*).

La sous-couche PMD est chargée de la modulation/démodulation, le codage et le décodage des signaux.

La sous-couche PLCP offre à la couche MAC un point de service (SAP) commun pour toutes les technologies de transmission définies pour le WLAN. Elle offre aussi à la couche MAC le signal CCA (*Clear Channel Assessment*) qui indique si le canal est en train d'être utilisé. Ce signal est utilisé par la couche MAC pour les méthodes d'accès au canal basées sur le « *Carrier Sense* » que nous décrirons ultérieurement.

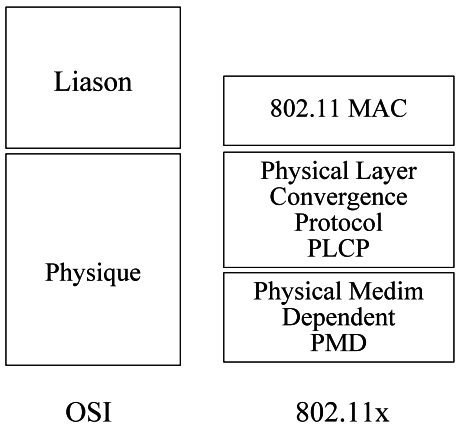


Figure 65: Division de la couche physique 802.11x en deux sous-couches

7.2.1 La norme 802.11b

Le réseau Wi-Fi 2 provient de la normalisation IEEE 802.11b sur la bande des 2,4 GHz (2,4–2,4835 GHz). D'autres équipements électroniques émettent à cette bande, notamment les réseaux Bluetooth et les fours micro-ondes. La méthode de spectre

étalé HR/DSSS (*High Rate Direct Sequence Spread Spectrum*) est utilisée pour obtenir une bonne protection contre des interférences avec d'autres équipements.

En ce début des années 2000, la norme IEEE 802.11b s'est imposée comme standard, et plusieurs millions de cartes d'accès réseau Wi-Fi 2 ont été vendues. Wi-Fi 2 a d'abord été déployé dans les campus universitaires, les aéroports, les gares et les grandes administrations publiques ou privées, avant de s'imposer dans les réseaux des entreprises pour permettre la connexion des PC portables et des équipements de type PDA.

Wi-Fi 2 travaille avec des stations de base dont la vitesse de transmission va jusqu'à 11 Mb/s et la portée de quelques dizaines de mètres. Pour obtenir cette valeur maximale de la porteuse, il faut que le terminal soit assez près de la station de base, à moins d'une vingtaine de mètres. Il faut donc, au moment de l'ingénierie du réseau, bien calculer le positionnement des différentes stations de base. La Table 15 résume les zones de couverture.

Table 15: Zones de couverture dans IEEE 802.11b

Débit	Portée
A l'intérieur des bâtiments	
11 Mb/s	50 m
5 Mb/s	75 m
2 Mb/s	150 m
1 Mb/s	200 m
A l'extérieur des bâtiments	
11 Mb/s	200 m
5 Mb/s	300 m
2 Mb/s	400 m
1 Mb/s	500 m

Aux États-Unis, 11 canaux sont disponibles dans une largeur de bande des 83,5 MHz tandis qu'en Europe, dès que la bande est entièrement libérée, 14 canaux d'une largeur de bande de 20 MHz chacun seront disponibles. Une station de base ne peut utiliser que trois fréquences au maximum, car l'émission demande une bande passante qui recouvre quatre fréquences (Figure 66). Pour cela, la station de base doit contenir trois cartes coupleurs Wi-Fi 2.

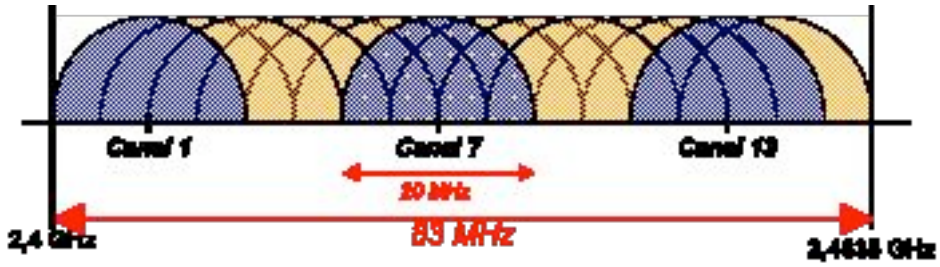


Figure 66: Utilisation de canaux dans IEEE 802.11b

Les fréquences peuvent être réutilisées régulièrement. De la sorte, dans une entreprise, le nombre de machines que l'on peut raccorder est très important et permet à chaque station terminale de se raccorder à haut débit à son serveur ou à un client distant (Figure 67).

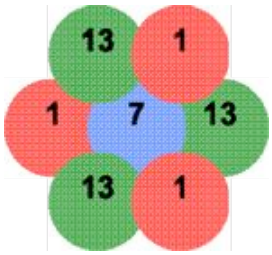


Figure 67: Réutilisation des canaux

7.2.2 La norme 802.11a

Wi-Fi 5 provient de la normalisation IEEE 802.11a sur la bande des 5 GHz. L'allocation des fréquences est différente pour l'Europe, les Etats-Unis et le Japon. La Figure 68 montre l'utilisation des fréquences en Europe.

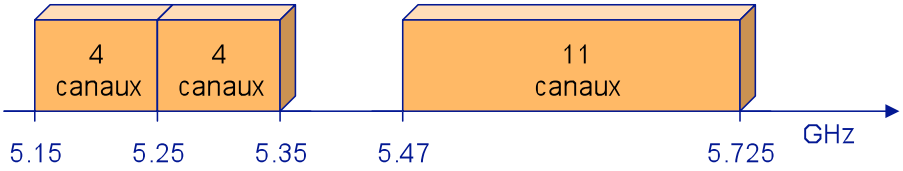


Figure 68: Utilisation des fréquences dans IEEE 802.11a

Les sous-bandes de 5.15-5.25 GHz, 5.25-5.35 GHz et 5.47-5.725 GHz sont autorisées en Europe. La bande est divisée en canaux de 20 MHz chacun, ce qui permet la colocation de 19 canaux séparés au sein d'un même espace. Contrairement à 802.11b, les canaux ne se chevauchent pas et peuvent donc être utilisé simultanément dans une même cellule.

Cette norme a pour origine des études effectuées dans le cadre de la normalisation HiperLAN de l'ETSI en ce qui concerne la couche physique. La couche MAC de l'IEEE 802.11b est en revanche conservée et donc différente de la couche équivalente dans HiperLAN qui est fondée sur ATM. Wi-Fi 5 n'est pas compatible avec Wi-Fi 2, les fréquences utilisées étant totalement différentes. Les fréquences peuvent toutefois se superposer si l'équipement qui souhaite accéder aux deux réseaux comporte deux cartes d'accès.

Pour la partie physique, les propositions suivantes ont été retenues pour Wi-Fi 5 :

- Fréquence de 5 GHz dans la bande UNII (*Unlicensed National Information Infrastructure*), une bande de fréquences sans licence aux États-Unis, c'est-à-dire qui ne demande pas l'obtention d'une licence d'utilisation.
- Modulation OFDM (*Orthogonal Frequency Division Multiplexing*) avec 52 porteuses, autorisant des performances excellentes en cas de chemins multiples.
- Huit débits échelonnés de 6 à 54 Mb/s. Le débit sélectionné par la carte d'accès dépend de la puissance de réception. Pour une distance de quelques mètres entre la carte d'accès et la station de base, la vitesse est de 54 Mb/s.

La distance maximale entre la carte d'accès et la station de base peut dépasser les 100 m, mais la chute du débit de la communication est fortement liée à la distance. Pour le débit de 54 Mb/s, la station mobile contenant la carte d'accès ne peut s'éloigner que de quelques mètres de la station de base. Au-delà, le débit chute très vite pour être approximativement équivalent à celui qui serait obtenu avec la norme 802.11b à 100 m de distance.

En réalisant de petites cellules, de façon que les fréquences soient fortement réutilisables, et compte tenu du nombre important de fréquences disponibles en parallèle jusqu'à 5), le réseau Wi-Fi 5 permet à plusieurs dizaines de clients par 100 m^2 de se partager entre 100 et 200 Mb/s. De ce fait, le réseau Wi-Fi 5 est capable de prendre en charge des flux vidéo de bonne qualité.

Wi-Fi 5 devrait permettre à de très nombreuses stations de travail et portables de se connecter automatiquement dans les entreprises qui en seront dotées. Les niveaux supérieurs au niveau MAC, c'est-à-dire à la couche gérant l'algorithme d'accès CSMA/CD, correspondent à celles que l'on rencontre dans les réseaux Ethernet.

7.2.3 La norme 802.11g

La norme IEEE 802.11g a été finalisée récemment et de l'équipement 802.11g est déjà disponible dans les magasins. Comme la norme 802.11b, 802.11g utilise la bande de fréquences des 2,4 GHz, mais avec un débit jusqu'à 54 Mb/s. La technique de modulation utilisée est celle de l'IEEE 802.11a, c'est-à-dire la modulation OFDM. L'avantage de cette solution par rapport à l'IEEE 802.11a est une portée supérieure. Un autre avantage est que les équipements 802.11g sont compatibles avec 802.11b, c'est-à-dire un point d'accès 802.11g est capable de communiquer avec des stations 802.11b.

7.2.4 Comment choisir la bonne norme

La Table 16 résume les paramètres ainsi que les avantages et inconvénients des différentes normes 802.11x.

Table 16: Résumé des caractéristiques des normes 802.11

Norme	Caractéristiques	Avantages	Inconvénients
802.11b	• Débit jusqu'à 11 Mb/s • Bande de 2.4 GHz • 3 canaux séparés	• Utilisée par la plupart des équipements • Prix faible • Bonne portée	• Débit faible • Interférence avec d'autres équipements dans la bande de 2.4 GHz • Peu de canaux utilisables simultanément
802.11g	• Débit jusqu'à 54 Mb/s • Bande de 2.4 GHz • 3 canaux séparés	• Bonne porté • Compatible avec 802.11b • Débit élevé • Prix moyen	• Interférence avec d'autres équipements dans la bande de 2.4 GHz • Peu de canaux utilisables simultanément
802.11a	• Débit jusqu'à 54 Mb/s • Bande de 5 GHz	• Pas d'interférences avec d'autres	• Porté plus faible • Coût plus élevé • Incompatible avec

	• 19 canaux séparés	équipements • Débit élevé • Beaucoup de canaux utilisables simultanément	802.11b

7.2.5 Les couches physiques

Les différentes couches physiques utilisent la méthode de modulation appelée « Spectre étalé » (*Spread Spectrum*). Cette modulation étale la puissance du signal à transmettre sur une bande de fréquence beaucoup plus large que nécessaire. Cette méthode sacrifie donc de la largeur de bande pour obtenir d'autres avantages. Ainsi, le signal transmis est beaucoup moins susceptible de bruit de transmission ou d'interférences avec d'autres transmissions dans la même bande de fréquence. Il en résulte un taux d'erreurs bit plus faible que dans une modulation « habituelle ».

7.2.5.1 FHSS (*Frequency Hopping Spread Spectrum*)

Cette couche physique utilise la bande de fréquences de 2,4 GHz. *Frequency hopping* appartient aux modulations spectre étalé. Le but original était de crypter les communications. En plus d'être un système de chiffrage efficace, cette méthode réduit les effets d'interférence et permet la coexistence de plusieurs réseaux dans la même zone.

L'émetteur et le récepteur communiquent en utilisant de manière séquentielle une série de fréquences qui changent rapidement et de manière pseudo-aléatoire et coordonnée.

La Figure 69 montre le principe utilisé.

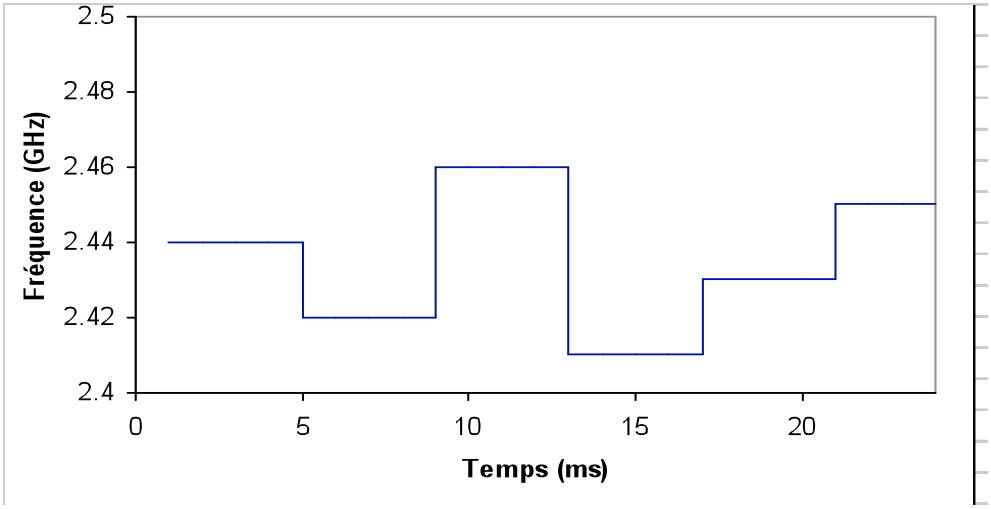


Figure 69: Fonctionnement de la méthode du *Frequency hopping*

Dans la figure, la transmission/réception se fait à 2,44 GHz pendant les premières 5 ms. Les stations font alors un saut simultané à la fréquence 2,42 GHz pour le prochain

intervalle de 5 ms, puis à 2,46 GHz, et ainsi de suite. Dans le cas où plus d'un réseau serait en opération dans la même zone de couverture, et que chaque réseau utiliserait une séquence de fréquences différente, les interférences et les problèmes de fading qui apparaissent à des fréquences seront minimisés.

Chaque changement de fréquence est appelé un *hop*. L'émetteur et le récepteur WLAN effectuent 79 hops synchronisés par seconde avec des séquences données par des séries pseudo aléatoires bien définies qui se trouvent dans la norme 802.11. La différence entre deux fréquences successives est d'au moins 6 MHz. La largeur de bande dans chaque fréquence est de 1 MHz.

La norme 802.11 spécifique, pour les systèmes FHSS, deux débits de transmission : 1 Mb/s et 2 Mb/s, ce dernier étant optionnel.

7.2.5.2 DSSS (*Direct Sequence Spread Spectrum*)

Direct Sequence Spread Spectrum est, comme FHSS, une technique de spectre étalé. Le principe est cependant très différent. Le signal qui représente la séquence de bits à transmettre est multiplié par une séquence binaire dite **séquence d'étalage**. Cette opération a pour effet l'élargissement de la bande passante du signal original. Au récepteur, on multiplie le signal de bande large par la même séquence pseudo aléatoire et on récupère ainsi le signal modulé original. Dans la norme 802.11, l'étalement s'effectue avec un code de Barker à 11 bits (appelés chips) par symbole à transmettre. Le code de Barker choisi est 10110111000. Le processus est illustré dans la Figure 70.

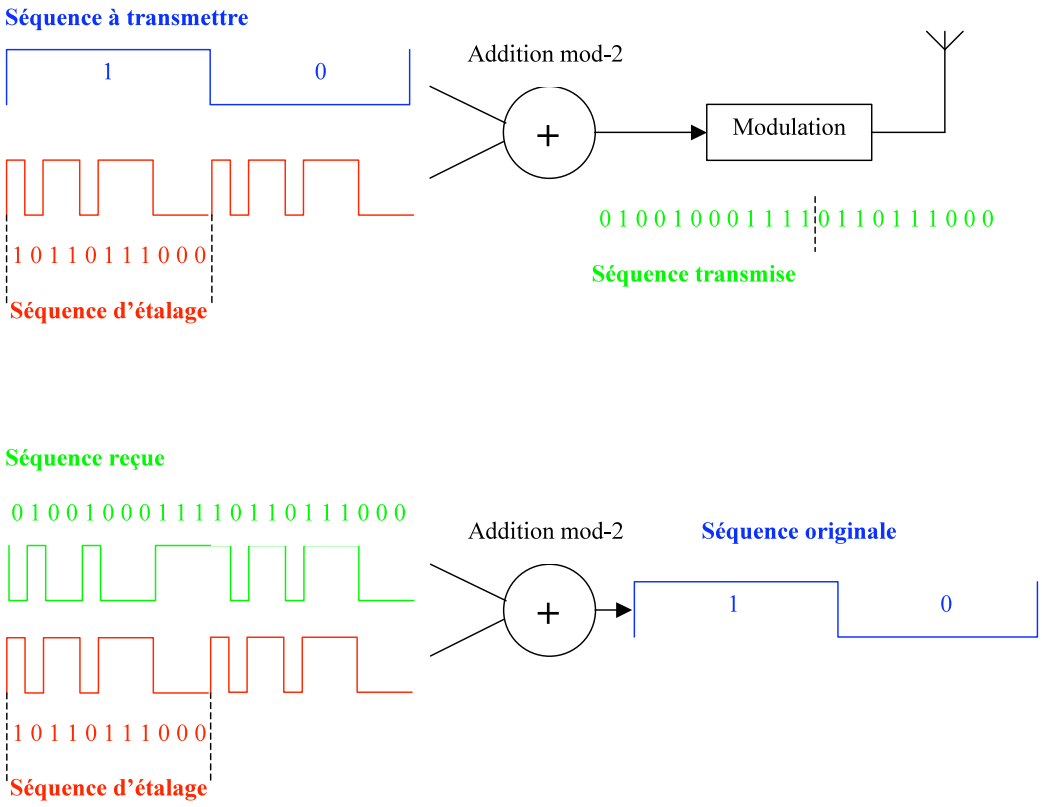


Figure 70: Illustration du principe de DSSS

Figure 71: Effet du spectre étalé sur des interférences

La norme 802.11b utilise une variante de cette méthode appelée High Rate DSSS (HR/DSSS) pour atteindre un débit allant jusqu'à 11 Mb/s.

7.2.5.3 OFDM (*Orthogonal Frequency Division Multiplexing*)

OFDM est également une technique de spectre étalé, est basée sur le multiplexage fréquentiel (FDM). L'idée de OFDM est de diviser le canal de transmission en plusieurs porteuses de repartir la séquence binaire à transmettre sur les différentes porteuses. Chaque porteuse ayant une largeur de bande faible, les interférences et d'autres problèmes de transmission radio sont ainsi diminués. La complexité de cette technique se situe dans le choix des fréquences des porteuses et des méthodes de modulation afin d'éliminer les interférences entre les différentes sous-canaux. L'orthogonalité signifie, qu'il n'y a aucune interférence entre les sous-canaux.

Cette technique est utilisée dans IEEE 802.11a avec 52 porteuses par canal, dont 48 porteuses de données et 4 porteuses de correction d'erreur (Figure 72).

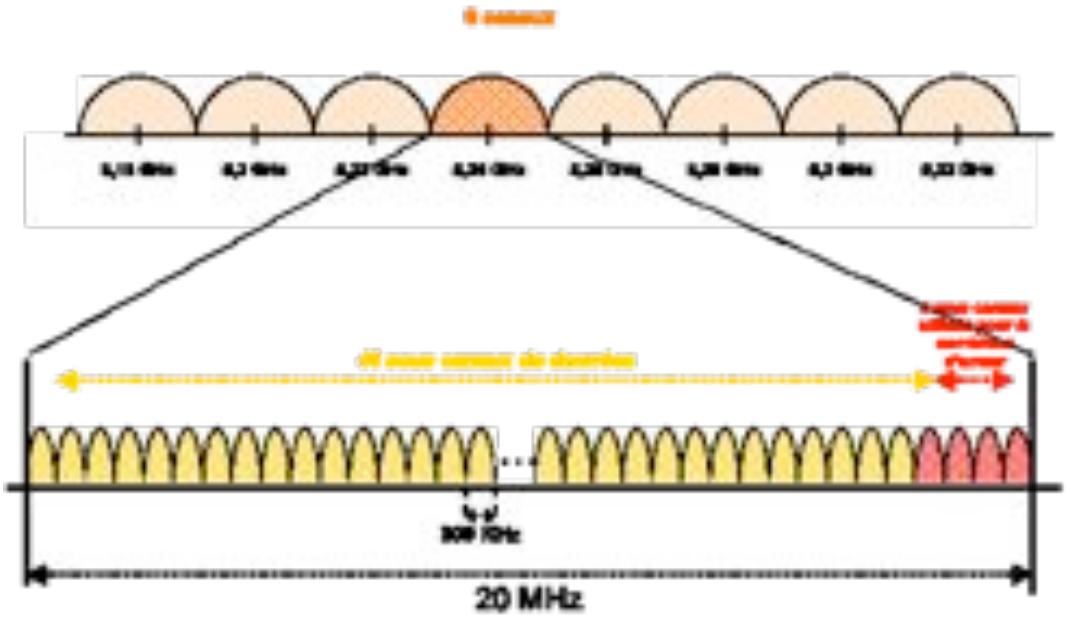


Figure 72: Division d'un canal en plusieurs sous-canaux dans OFDM (802.11a)

7.2.6 La couche liaison

La couche liaison de données du protocole 802.11 est composée essentiellement de deux sous-couches, LLC (*Logical Link Control*) et MAC. La couche LLC utilise les mêmes propriétés que la couche LLC 802.2. Il est de ce fait possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE. La couche MAC, quant à elle, est spécifique de l'IEEE 802.11.

Le rôle de la couche MAC 802.11 est assez similaire à celui de la couche MAC 802.3 du réseau Ethernet terrestre, puisque les terminaux écoutent la porteuse avant d'émettre. Si la porteuse est libre, le terminal émet, sinon il se met en attente.

Cependant, la couche MAC 802.11 intègre un grand nombre de fonctionnalités que l'on ne trouve pas dans la version terrestre.

Les fonctionnalités nécessaires pour réaliser un accès sur une interface radio sont les suivantes :

- procédures d'allocation du support
- adressage des paquets
- formatage des trames
- contrôle d'erreur CRC (*Cyclic Redundant Check*)
- fragmentation-réassemblage.

7.2.7 Méthodes d'accès au canal

L'une des particularités du standard est qu'il définit **deux méthodes** d'accès fondamentalement différentes au niveau de la couche MAC.

DCF. La première est la **DCF** (*Distributed Coordination Function*), qui correspond à une méthode d'accès assez similaire au réseau traditionnel supportant le best-effort. La DCF a été conçue pour prendre en charge le transport de données asynchrones, dans lequel tous les utilisateurs qui veulent transmettre des données ont une chance égale d'accéder au support. Elle utilise deux mécanismes :

- CSMA/CA : *Carrier Sense Multiple Access / Collision Avoidance*
- Des trames de réservation RTS et CTS.

PCF. La seconde méthode d'accès est la **PCF** (*Point Coordination Function*). Fondée sur l'interrogation à tour de rôle des terminaux, ou *polling*, contrôlée par le point d'accès, la méthode PCF est conçue essentiellement pour la transmission de données sensibles, qui demandent une gestion du délai utilisé pour les applications temps réel, telles que la voix ou la vidéo.

Les WLAN basés sur infrastructure peuvent utiliser soit la DCF soit la PCF. Les réseaux ad-hoc utilisent la DCF.

7.2.7.1 CSMA/CA

En tenant compte de ces spécificités, Wi-Fi utilise un protocole légèrement modifié par rapport au CSMA/CD, appelé CSMA/CA. Ethernet, qui utilise CSMA/CD détecte des collisions de transmissions. Pour les réseaux locaux sans fil, la détection de collisions n'est pas possible.

Dans Wi-Fi, le temps est découpé en tranches, qui correspondent chacune à un time-slot. Contrairement au time-slot utilisé dans l'ALOHA, qui correspond à la durée minimale de transmission d'une trame, le time-slot utilisé dans Wi-Fi est un peu plus petit que la durée de transmission minimale d'une trame. Il est utilisé pour définir les intervalles IFS ainsi que les temporisateurs pour les différentes stations. Son implémentation est différente pour chaque couche physique.

L’accès au support est contrôlé par l'utilisation d'espaces inter-trames, ou IFS (*InterFrame Spacing*), qui correspond à l'intervalle de temps entre la transmission de deux trames. Les *intervalles* IFS sont des périodes d'inactivité sur le support de transmission. Les valeurs des différents IFS sont calculées par la couche physique.

Le standard définit trois types d'IFS.

SIFS (*Short Initial interframe Space*), le plus petit des IFS, est utilisé pour séparer les transmissions au sein d'un même dialogue (envoi de données, ACK, etc.). Il y a toujours une seule station pour transmettre à cet instant, ayant donc la priorité sur toutes les autres stations.

PIFS (PCF IFS), utilisé par le point d'accès pour accéder avec priorité sur le support par rapport, aux stations du réseau. Le PIFS correspond à la valeur du SIFS, auquel on ajoute un slot-time.

DIFS (DCF IFS), utilisé lorsqu'une station veut commencer une nouvelle transmission. Le DIFS correspond à la valeur du PIFS, à laquelle on ajoute un slot-time.

Les valeurs des différents intervalles sont montrées dans la Table 17.

Table 17: Intervalles IFS des différentes normes

Intervalle / Norme	802.11	802.11a	802.11b
Slot time	50 µs	9 µs	20 µs
SIFS	28 µs	16 µs	10 µs
PIFS	78 µs	25 µs	30 µs
DIFS	128 µs	34 µs	50 µs

Une station source voulant transmettre des données écoute le support. Si aucune activité n'est détectée pendant une période de temps correspondant à un DIFS, la station source transmet ses données immédiatement.

Si les données envoyées sont reçues intactes - la station destination vérifiant le CRC de la trame -, la station destination attend pendant un temps équivalent à un SIFS et émet un ACK pour confirmer la bonne réception des données. Si l’ACK n'est pas détecté par la station source ou si les données ne sont pas reçues correctement ou encore si l'ACK n'est pas reçu correctement, on suppose qu'une collision s'est produite, et la trame est retransmise.

Lorsque la station source transmet ses données, les autres stations mettent à jour leur NAV, en incluant le temps de transmission de la trame de données, le SIFS et FACK.

La Figure 73 illustre le processus de transmission d’une trame entre une station A et une station B en mode infrastructure. La trame est d’abord reçue par le point d’accès qui la fait suivre vers la station B. Il est à noter que chaque trajet de la transmission doit être acquitté.

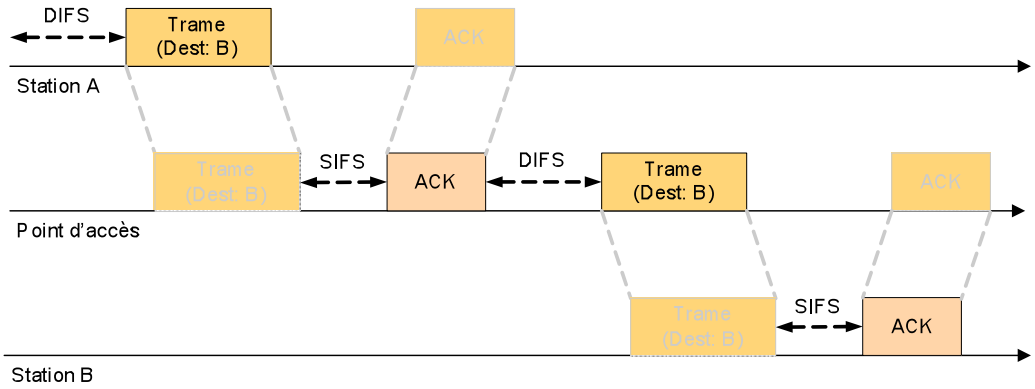


Figure 73: Principe de la transmission d'une trame en 802.11

Collision Avoidance

Ce principe décrit ci-dessus correspond à la méthode CSMA persistant, discuté au début de ce chapitre. Or, nous savons que cette méthode a un défaut qui dégrade les performances : si plusieurs station attendent la libération du canal, il y aura forcement une collision. Pour éviter ce problème est améliorer les performances, la couche MAC introduit une extension de l'algorithme de base : l'évitement de collisions (*congestion avoidance*).

Lorsque une station veut transmettre, elle attendant jusqu'à ce qu'elle ait vu la canal libre pendant un intervalle de temps DIFS. Ensuite, au lieu de commencer tout de suite la transmission, est commence l'attente d'un délai aléatoire, et cela indépendamment du fait qu'elle ait trouve le canal libre ou occupé au début de l'écoute.

Le délai aléatoire est calculé comme le produit du slot time avec un nombre entier aléatoire, choisi dans l'intervalle [0, CW]. CW (Contention Window) a initialement la valeur CWmin et double avec chaque collision lors d'une tentative de transmission jusqu'à la valeur CWmax. Après une transmission réussie, CW est remise à CWmin.

Les valeurs de CWmin et CWmax dépendent de la variante 802.11 utilisée. Dans 802.11b, CWmin = 31 et CWmax = 1023.

Lorsque le support est libre, les stations décrémentent leur temporisateur jusqu'à ce que le support soit occupé ou que le temporisateur atteigne la valeur 0. Si le temporisateur n'a pas atteint la valeur 0 et que le support soit de nouveau occupé, la station bloque le temporisateur. Dès que le temporisateur atteint la valeur 0, la station transmet sa trame. Si deux ou plusieurs stations atteignent la valeur 0 au même instant, une collision se produit, et chaque station doit régénérer un nouveau temporisateur.

Cette méthode est donc similaire au backoff exponentiel que nous avons vu dans Ethernet CSMA/CD. La grande différence se trouve dans le fait qu'en CSMA/CD, le backoff exponentiel est utilisé seulement après une collision. En CSMA/CA, une station doit attendre un délai aléatoire toujours avant de transmettre une trame. La seule exception est quand une station veut transmettre une trame après avoir été silencieuse pendant une durée prolongée. Dans ce cas, elle aura déjà attendu un délai aléatoire après la transmission de la trame précédente. Si elle trouve le canal libre

pendant le temps DIFS, elle pourra toute de suite transmettre la trame, sans à nouveau attendre un délai aléatoire.

En résumé, le backoff dans CSMA/CA est utilisé

- quand le canal est occupé lors de l'écoute
- après une transmission réussie
- après chaque retransmission.

Grâce à cet algorithme, les stations ont la même probabilité d'accéder au support, car chaque station doit, après chaque transmission, accéder à nouveau au support. Son seul inconvénient est de ne pas garantir un délai minimal et donc de compliquer la prise en charge d'applications temps réel telles que la voix ou la vidéo.

7.2.7.2 La réservation avec RTS/CTS

La technique de réservation essaie de combattre deux problèmes :

- les collisions et retransmissions de trames très longues
- l'effet de la station cachée.

Une station émettrice n'étant pas capable de détecter une collision, elle émet toujours une trame complète, mais s'il y a collision. Pour des trames longues, ceci gaspille de la capacité du canal. L'idée est de transmettre d'abord une trame courte pour réserver le canal et ensuite la trame longue. La trame courte peut subir une collision, celle-ci gaspillant cependant moins de temps qu'une collision de la trame longue.

Le problème de la station cachée peut être compris à l'aide de la Figure 74.

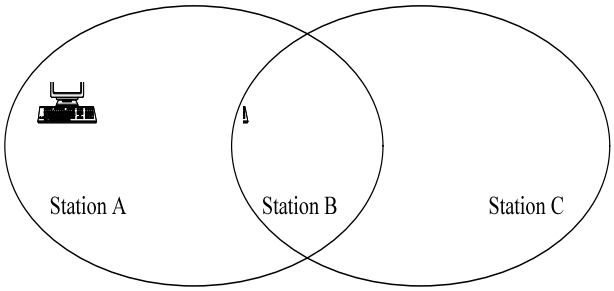


Figure 74: Problème de la station cachée

Considérez la situation suivante: Les stations A et C sont trop loin pour que les transmissions de l'une soient détectées par l'autre mais assez proches de la station B pour que celle-ci puisse les détecter. La station A a une trame à transmettre à la station B. Elle attend DIFS et, si elle ne détecte pas d'activité dans le canal, elle commence à transmettre. Si la station C a, elle aussi, des données pour la station B, elle les transmettra aussi pensant incorrectement que le canal est inactif. Ceci produit une collision à la station B.

Le problème de la station cachée est donc qu'une station ne peut pas détecter avec certitude si une autre transmission est déjà cours.

Voyons maintenant comment la technique d'accès RTS/CTS entreprend d'éviter ce problème.

La station désirant transmettre attend que le canal soit inactif pendant un intervalle DIFS et son temps d'attente aléatoire si nécessaire. Elle transmet alors une trame **RTS** (*Request to Send*) qui a pour but la réservation du canal pendant la duré totale de la transmission. La trame RTS contient alors des informations sur

- la station source,
- la station à laquelle les données seront destinées et
- la durée totale de la transmission, y compris les échanges de trames de contrôle.

Chaque station utilise ces informations pour initialiser un temporisateur NAV (*Network Allocation Vector*) qui indique le moment auquel la station peut à nouveau essayer d'accéder au canal (voir la Figure 75). Il est mis à jours grâce à l'information contenue dans les trames RTS et CTS.

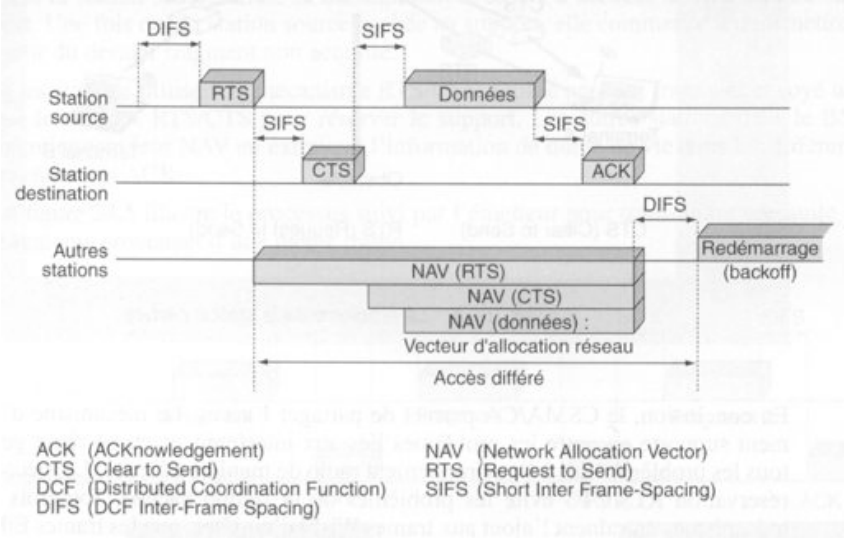


Figure 75: Utilisation de RTS et CTS

Si le récepteur détecte le RTS, il attend un intervalle SIFS et envoie une trame de contrôle **CTS** (*Clear to send*). Comme la trame RTS, la trame CTS contient l'identité de la station émettrice et du récepteur aussi bien que la durée de transmission recalculée pour tenir compte du temps déjà écoulé. Les stations qui reçoivent le CTS ne sont pas forcément les mêmes qui ont reçu le RTS. En effet, le groupe de stations qui détectent le CTS comprend aussi les stations cachées. Ces stations réservent le temps de la transmission à l'aide de leurs NAVs.

La station émettrice attend SIFS avant d'émettre la trame de données. Celle-ci est reçue par la station réceptrice qui, à son tour, répond avec une quittance (ACK) après SIFS. Si la quittance est corrompue ou elle n'arrive pas chez l'émetteur, celui-ci doit effectuer une retransmission pendant le prochain cycle.

Les stations peuvent choisir d'utiliser le mécanisme RTS/CTS ou non, ou de ne l'utiliser qu lorsque la longueur de la trame à envoyer excède un certain seuil.

En conclusion, le CSMA/CA permet de partager l'accès. Le mécanisme d'acquittement supporte en outre les problèmes liés aux interférences et, en règle générale, à tous les problèmes liés à l'environnement radio de manière efficace. Le mécanisme de réservation RTS/CTS évite les problèmes de la station cachée. Toutefois tous ces mécanismes entraînent l'ajout aux trames Wi-Fi d'en-têtes, que les trames Ethernet ne possèdent pas. C'est pourquoi les réseaux Wi-Fi montrent toujours des performances plus faibles que les réseaux locaux Ethernet.

7.2.7.3 Polling

Contrairement aux méthodes CSMA/CA et RTS/CTS, le schéma PCF (*Point Coordination Function*) que nous allons décrire peut être utilisé pour garantir une qualité de service. PCF est optionnelle dans les normes 802.11.

Cette méthode d'accès au canal requiert d'un point d'accès (AP) qui joue le rôle de coordinateur ponctuel (*point coordinator*). Ceci implique que les réseaux ad hoc ne peuvent pas l'utiliser.

Le coordinateur divise le temps d'accès en super-trames. Les super-trames consistent en une période sans contention qui est utilisée pour le polling et une période de contention qui est utilisée pour les autres méthodes d'accès.

Le coordinateur attend que le canal soit inactif pendant PIFS avant de transmettre une trame destinée à une station 1. Étant donné que PIFS est plus court que DIFS, aucune autre station ne peut accéder au canal avant le coordinateur. La station 1 peut répondre après SIFS. Le coordinateur attend alors SIFS et envoie des données à la deuxième station. Celle-ci, si elle a des données à transmettre, les envoie après SIFS. Le coordinateur suit la même procédure avec toutes les stations, une par une. Si une station n'a rien à transmettre, le coordinateur attend PIFS avant de continuer avec la prochaine station. Une fois toutes les stations contactées, le coordinateur envoie une trame CF-End qui marque la fin de la période sans contention et le début de la période de contention.

Le schéma est illustré sur la Figure 76.

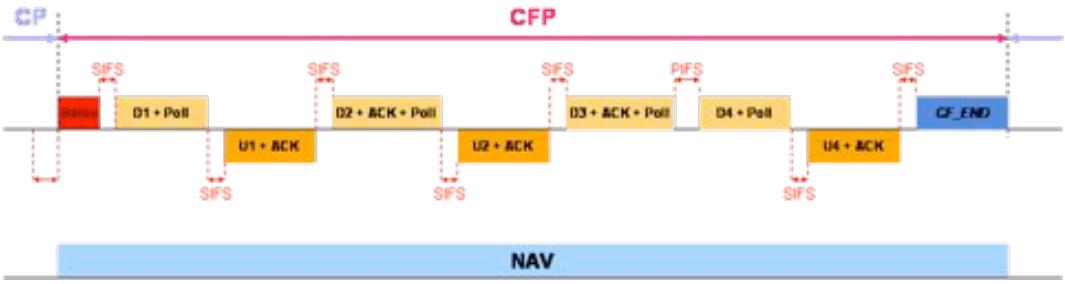


Figure 76: Mécanisme PCF

7.2.7.4 Fragmentation

Nous venons d'introduire le protocole qui permet à une station d'accéder au support hertzien pour émettre sa trame. Une question qui se pose concerne la taille de la trame. La fragmentation d'une trame en plusieurs trames de taille inférieure accroît la fiabilité de la transmission. Cette solution a pour effet de réduire le besoin de

retransmettre des données dans de nombreux cas et d'augmenter ainsi les performances globales du réseau. La fragmentation est utilisée notamment dans les liaisons radio, dans lesquelles le taux d'erreur est important. En effet, plus la taille de la trame est grande, plus elle a de chance d'être corrompue.

Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle. Le support n'est libéré qu'après que tous les fragments soient transmis avec succès ou si la station source ne réussit pas à recevoir l'acquittement d'un fragment transmis.

La station destination acquitte chaque fragment reçu avec succès en envoyant un ACK à la station source. La station source garde le contrôle du support pendant toute la durée de la transmission d'une trame en attendant un temps SIFS après la réception d'un ACK ou après la transmission d'un fragment. Si un ACK n'est pas correctement reçu, la station source arrête la transmission et essaie d'accéder de nouveau au support. Une fois que la station source accède au support, elle commence à transmettre à partir du dernier fragment non acquitté.

Si les stations utilisent le mécanisme RTS/CTS, seul le premier fragment envoyé utilise les trames RTS/CTS pour réserver le support. Les autres fragments contiennent, eux aussi, une nouvelle réservation pour les fragments suivants. Les autres stations dans le BSS maintiennent leur NAV en extrayant l'information de durée de vie dans les différents fragments et ACK.

La Figure 77 illustre le processus suivi par l'émetteur pour transmettre une suite de fragments provenant d'une même trame.

La trame est assemblée lorsque la station destination a reçu tous les fragments de la station source.

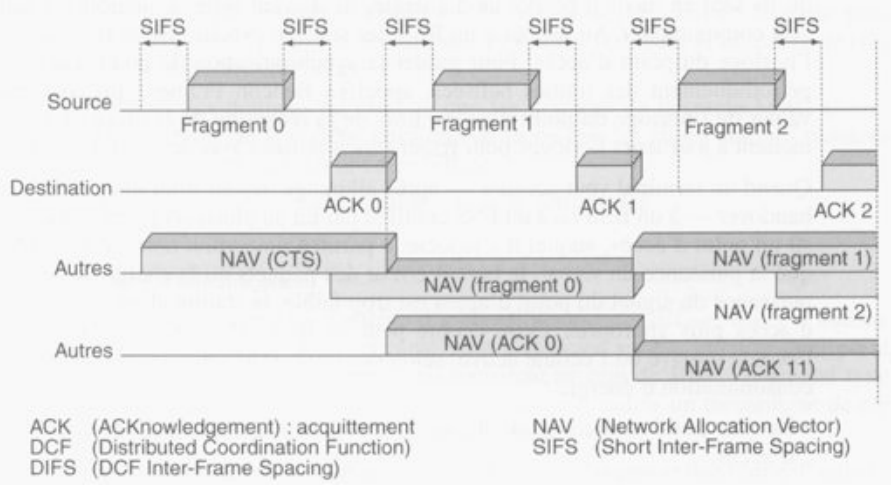


Figure 77: Transmission d'une trame fragmentée

7.2.8 Les trames Wi-Fi

Les paquets IP composés dans les terminaux du réseau sans fil doivent être transmis sur le support hertzien. Pour cela, ils doivent être placés dans une trame Ethernet. De plus, pour contrôler et pour gérer la liaison, il est nécessaire d'avoir des trames spécifiques. Il existe pour cela trois types de trames :

- trames de données, utilisées pour la transmission de données utilisateur.
- trames de contrôle, utilisées pour contrôler l'accès au support (RTS, CTS, ACK).
- trames de gestion, utilisées pour les associations ou les dés-associations d'une station avec un point d'accès, ainsi que pour la synchronisation et l'authentification.

Toutes les trames Wi-Fi sont composées de la manière illustrée à la Figure 78.

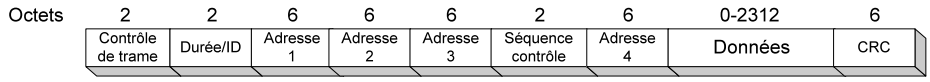


Figure 78: Trame Wi-Fi

Les adresses 1 et 2 identifient toujours le destinataire immédiat et la source la plus récente de la trame. La signification des autres champs d'adresses peut varier selon la trame.

La couche physique, ou plus précisément la sous-couche PLCP ajoute également un en-tête. Le format exact de l'en-tête dépend de la couche physique utilisée. La Figure 79 montre l'encapsulation en 802.11b.

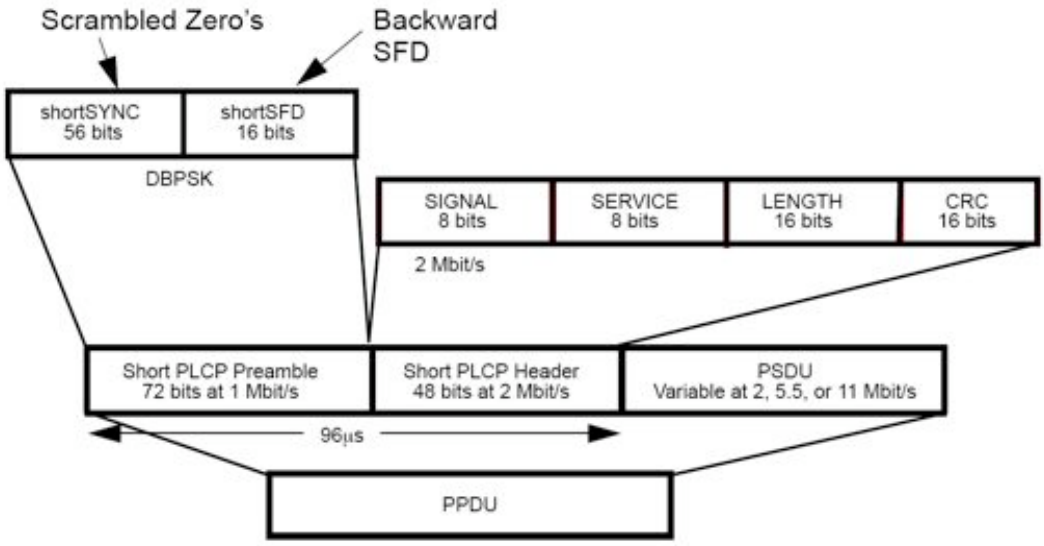


Figure 79: En-tête PLCP de 802.11b (source : norme 802.11)

Le préambule contient les deux séquences suivantes :

- Synch, de 56 bits alternant 0 et 1, qui est utilisée par le circuit physique pour sélectionner l'antenne à laquelle se raccorder.
- SFD (*Start Frame Delimiter*), une suite de 16 bits, 0000 1100 10 11 110 1, utilisée pour définir le début de la trame.

L'en-tête PLCP (*Physical Layer Convergence Protocol*) contient les informations logiques suivantes utilisées par la couche physique respective pour décoder la trame.

Il est à noter que le préambule PLCP est toujours transmis à 1 Mb/s et l'en-tête PLCP à 2 Mb/s. La durée des données PLCP est donc toujours de 96 µs. Les données de la sous-couche MAC sont transmises avec un débit jusqu'à 11 Mb/s, selon la qualité du lien radio. La transmission du préambule et de l'en-tête PLCP à 1 et 2 Mb/s permet la comptabilité avec l'ancienne norme 802.11 qui travaillait à 2 Mb/s. Même si une station 802.11 n'est pas capable de recevoir correctement les données MAC, il peut interpréter les données PLCP et n'interférera pas avec la transmission.

7.2.9 Débit de transmission effectif

Le débit de transmission effectif à travers un lien WLAN est bien inférieur au débit de la couche physique, comme 11 Mb/s pour 802.11b et 54 Mb/s pour 802.11a/g. Afin de calculer le maximum du débit effectif, visible à la couche IP, on doit tenir compte :

- des en-têtes de la couche MAC et de la couche physique
- des délais avant la transmission d'un trame (DIFS, Backoff),
- des délais à cause de l'acquittement (SIFS, transmission de l'acquittement).

Un calcul montre, que le débit effectif dépend fortement de la taille des paquets encapsulés. La Table 18 résume les résultats pour différentes tailles de paquets.

Table 18: Débit effectif des différentes norms WLAN, vu de la couche IP

Standard	Débit max (PHY)	Débit max effectif	
		Paquet de 64 octets	Paquet de 1500 octets
802.11b	11 Mb/s	0.8 Mb/s	7.1 Mb/s
802.11g/a	54 Mb/s	1.3 Mb/s	20 Mb/s

7.2.10 Fonctions avancées

La norme définie des groupes de fonctions avancées :

- Synchronisation
- Power management
- Roaming
- Management Information base (MIB)

Synchronisation. Chaque nœud dans 802.11 maintient une horloge interne. La norme définie la TSF (*timing synchronisation function*) pour synchroniser les horloges de tous les nœuds. Dans un BSS, la synchronisation se fait par le biais du signal *Beacon* (signal phare). Ce signal est quasi-périodique et il contient l'information du temps exacte où la trame a été envoyée, l'identification du BSS et d'autres informations de management. Chaque nœud utilise le temps donné par le signal phare pour ajuster son horloge locale.
Pour les réseaux ad hoc la situation est un peu plus compliquée. Chaque fois que l'intervalle de phare (*beacon interval*) s'écoule, toutes les stations tentent de

transmettre un signal phare avec leur horloge pour référence. Puisque les stations transmettent le signal phare en utilisant la méthode CSMA/CA d'accès au canal, seulement une station gagne normalement. Les stations ajustent leurs horloges et elles suppriment leurs signaux phares pour le reste de cet intervalle.

Power management. La gestion de l'utilisation de l'énergie est essentielle pour le WLAN où les stations mobiles utilisent des piles comme sources. Afin d'épargner l'énergie des piles, 802.11 définit deux états pour une station : *sleep* et *awake* (dormante et réveillée). La norme permet aux stations qui choisissent d'opérer en mode *power-save* d'éteindre leur transmetteur et récepteur et d'entrer dans l'état dormant. Les stations doivent se réveiller périodiquement pour recevoir les trames destinées à elles et qui ont été gardées dans des zones tampon soit par les stations sources (ad-hoc) soit par le point d'accès (réseaux basés sur infrastructure).

Roaming. Le standard 802.11 ne définit pas comment le roaming est fait, mais en définit cependant les règles de base. L'itinérance donne la possibilité de passer d'un BSS à un autre sans perdre la connexion. Une procédure est suggérée dans 802.11 : Lorsqu'une station se rend compte que sa liaison avec le point d'accès avec lequel elle est associée n'est plus de bonne qualité, elle fait un scanning actif avec des trames « *probe request* » pour chercher d'autres points d'accès. Si elle reçoit une ou plusieurs trames « *probe response* », elle transmet une trame de re-association à un des points d'accès. Si elle reçoit une réponse positive (trame « *reassociation response* »), elle a trouvé un nouveau BSS. Le nouveau point d'accès est chargé d'informer l'ancien point d'accès à travers le DS.

7.2.11 Sécurité

La sécurité est le premier souci de ceux qui déploient les réseaux locaux sans fil. Dans les réseaux sans fil, le support est partagé. Tout ce qui est transmis et envoyé sur le support peut donc être intercepté. Le principal, pour les utilisateurs, est d'être sûr qu'un intrus ne pourra pas :

- accéder aux ressources du réseau en utilisant le même équipement sans fil
- capturer le trafic du réseau sans fil (écoute clandestine)

7.2.11.1 Le protocole WEP

Dans l'intention de permettre aux réseaux sans fil d'avoir un niveau de sécurité similaire aux réseaux fixes, le groupe de travail IEEE 802.11 a inclus dans la première norme 802.11 le protocole **WEP** (*Wired Equivalent Privacy*), dont les mécanismes s'appuient sur le chiffrage des données et l'authentification des stations. Ce protocole illustre bien les dangers de la conception d'un protocole de sécurité par des non-spécialistes en comité fermé. Le protocole WEP a plusieurs failles de sécurité qui permettent à un intrus équipé d'un ordinateur avec carte WLAN et de quelques logiciels disponibles sur Internet de décrypter le trafic d'un réseau en quelques heures.

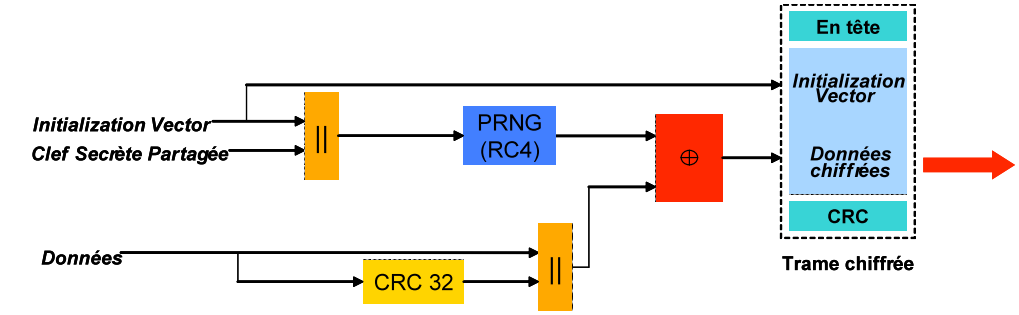
Les problèmes majeurs du protocole WEP sont :

- Authentification faible: usurpation d'identité
- Contrôle d'intégrité faible: modification, injection, reroutage des données

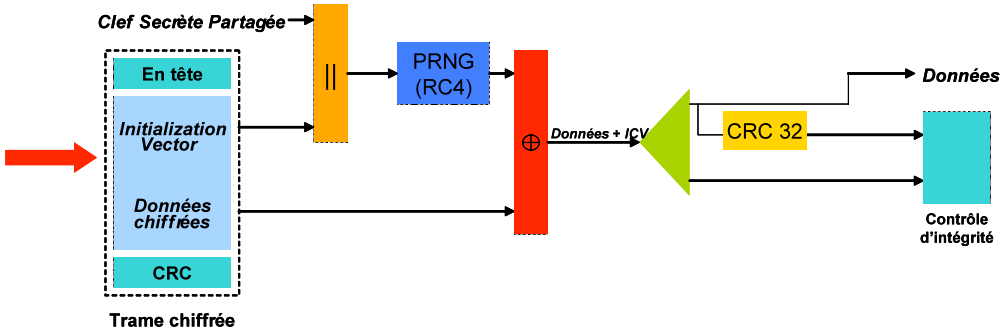
- Chiffrement faible: décryptage des données, récupération de la clé secrète.

Pour empêcher l'écoute clandestine sur le support, le protocole WEP utilise un algorithme de chiffrement des données. Chaque terminal possède une clé secrète partagée sur 40 ou 104 bits. Cette clé est concaténée avec un code de 24 bits, l'IV (*Initialisation Vector*), qui est modifié à chaque transmission d'une trame. La clé en résultat de 64 ou 128 bits est placée dans un générateur de nombre aléatoire, appelé PRNG (RC4) venant de l'algorithme de chiffrage RSA (Rivest Shamir Adelman). Ce générateur produit une séquence d'octets pseudo-aléatoires avec la même longueur que les données à chiffrer. Les données de la trame sont chiffrées en effectuant l'opération XOR (OR exclusif) entre chaque octet de données et un octet de la séquence pseudo-aléatoire. Une fois chiffrée, les données sont encapsulées dans une trame MAC. La trame MAC contient aussi le Vecteur d'Initialisation utilisée pour chiffrer la trame, ensemble avec la clé secrète. L'IV est doit être envoyé au destinataire comme il change pour chaque trame. Il est envoyé en clair, mais sans la clé secrète il est sans valeur pour un intrus. Pour le déchiffrage, l'IV est concaténé à la clé secrète et la séquence résultats sert à nouveau de clé pour le générateur d'octets pseudo-aléatoires RC4. Le destinataire retrouve alors la même séquence pseudo-aléatoire comme l'émetteur et peut ainsi déchiffrer les données contenues dans la trame.

Le schéma de l'algorithme de cryptage et de décryptage est montré à la Figure 80.



a) Algorithme de chiffrement



b) Algorithme de déchiffrement

Figure 80: Algorithme de chiffrement et de déchiffrement dans WEP

Le chiffrement des données ne protège que les données de la trame MAC et non l'en-tête de façon que les autres stations puissent toujours écouter les trames qui ont été chiffrées.

Il y a plusieurs failles de sécurité de cet algorithme :

- L'IV ayant 24 bits, il n'y a que 16 moi d'IV différents. Les IV se répètent alors au bout de quelques heures sur un réseau WLAN très chargé. Si l'intrus connaît le texte clair du message et le message chiffré, il peut calculer la séquence pseudo-aléatoire qui a été utilisée pour chiffrer le message. Cela lui permet d'établir un dictionnaire avec la séquence pseudo-aléatoire pour chaque IV. Lorsqu'il voit une autre trame avec le même IV il peut la déchiffrer (attaque par dictionnaire).
- Le vecteur d'initialisation représente les premiers bytes de la clé RC4. L'algorithme RC4 a une faiblesse (connue !) pour certains vecteurs d'initialisation (IV faibles). Si l'on connaît les premiers bytes de la clé RC4, on peut trouver le prochain byte à partir du premier byte de la séquence aléatoire générée par RC4. Cette attaque est mise en œuvre par les logiciels comme Airsnort ou WEPCrack qui sont capables d'obtenir la clé secrète en quelques heures.
- Le code correcteur CRC-32 est linéaire, c'est-à-dire CRC(M1)+CRC(M2) = CRC(M1 + M2). Sans connaissance du chiffrement un intrus peut alors facilement modifier le message et ensuite créer un nouveau CRC valable pour le message chiffré. Le destinataire du message ne peut pas détecter que le message a été modifié.

Authentification

Le protocole WEP définit également une méthode d'authentification d'un client auprès d'un AP. Les techniques d'authentification utilisées sont de deux sortes

- Open System Authentication
- Shared Key Authentication

Le premier type concerne un système d'authentification par défaut. Il n'y a aucune authentification explicite, et un terminal peut s'associer avec n'importe quel point d'accès et écouter toutes les données qui transitent au sein du BSS. Le second type fournit un meilleur système d'authentification puisqu'il utilise un mécanisme de clé secrète partagée. Ce mécanisme fonctionne en quatre étapes :

1. Une station voulant s'associer avec un point d'accès lui envoie une trame d'authentification.
2. Lorsque le point d'accès reçoit cette trame, il envoie à la station une trame contenant 128 bits d'un texte aléatoire généré par l'algorithme WEP.
3. Après avoir reçu la trame contenant le texte, la station la copie dans une trame d'authentification et la chiffre avec la clé secrète partagée avant d'envoyer le tout au point d'accès.
4. Le point d'accès déchiffre le texte chiffré à l'aide de la même clé secrète partagée et le compare avec celui qui a été envoyé plus tôt. Si le texte est identique, le point d'accès lui confirme son authentification, sinon il envoie une trame d'authentification négative.

La Figure 81 décrit les quatre étapes suivies pour l'authentification d'une station que nous venons de détailler.

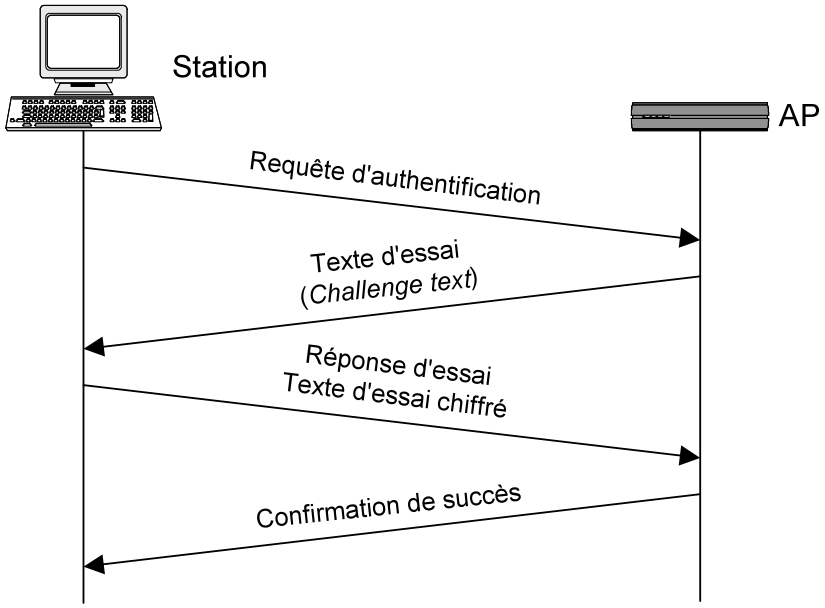


Figure 81: Mécanisme d'authentification d'une station

A nouveau, l'algorithme d'authentification par clé secrète partagée présente une faille de sécurité. Le texte d'essai et d'abord envoyé en clair, puis chiffré. Un intrus qui intercepte les deux messages peut calculer l'opération XOR entre les deux et ainsi trouver la séquence pseudo-aléatoire générée par RC4. Cette authentification facilite alors considérablement une attaque par dictionnaire, comme expliquée ci-dessus.

L'utilisation de l'authentification par clé secrète est donc déconseillée.

7.2.11.2 Améliorations de la sécurité dans WLAN

Plusieurs solutions existent aujourd'hui qui remplacent WEP et améliorent la sécurité dans un réseau WLAN.

WEP+

WEP+ est une solution ad-hoc adoptée par les constructeurs d'équipements WLAN. Elle consiste simplement à éviter l'utilisation de vecteurs d'initialisation faibles lors du chiffrement. Cette solutions peut être réalise très facilement en modifiant par exemple le pilote d'une carte WLAN. Le problème de cette solution est que les vecteurs d'initialisation faibles ne sont pas tous connus. Lorsqu'un nouveau IV faible est découvert, tous les équipements WLAN devraient être mis à jour.

L'authentification 802.1X

Le protocole 802.1x utilise un serveur RADIUS afin d'authentifier chaque utilisateur individuellement. Lorsqu'un nouveau client WLAN s'associe à un AP, tout trafic depuis ou vers le client reste bloqué jusqu'à l'authentification correcte. Le client commence alors une procédure d'authentification, basée sur le protocole EAP (*Extensible Authentication Protocol*), comme montrée à la Figure 82.

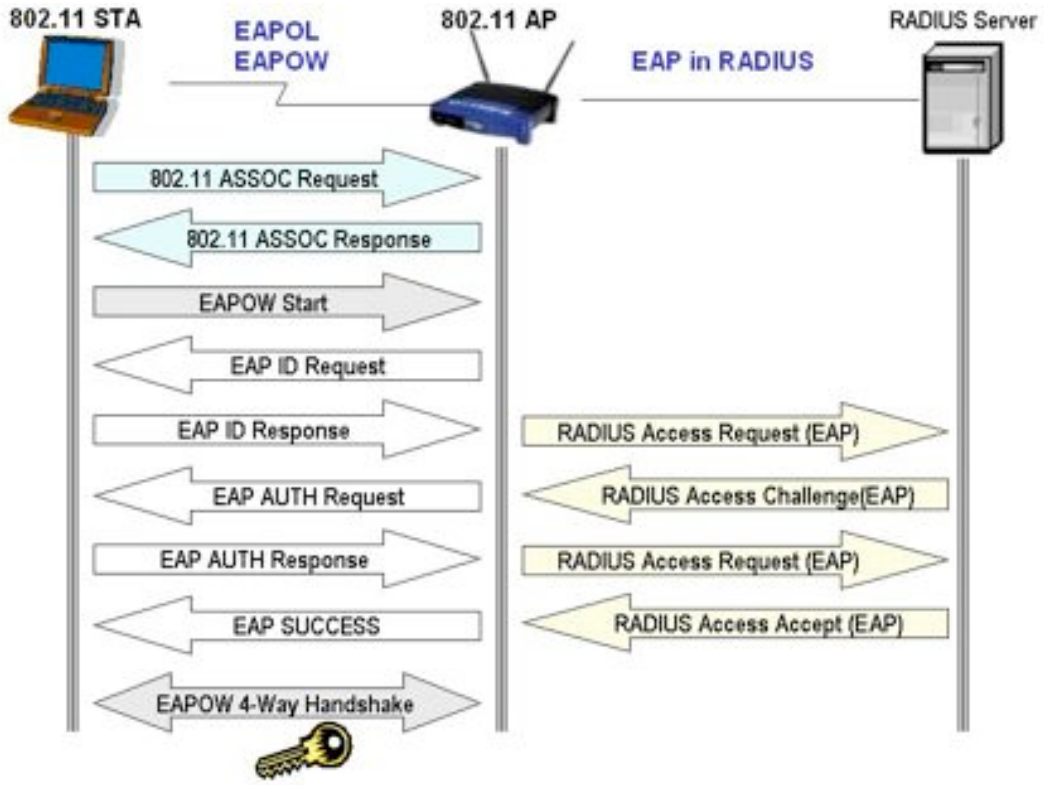


Figure 82: Authentification 802.1X

L'AP joue le rôle d'un relais entre le client et le serveur radius. Le serveur RADIUS demande une authentification du client, par exemple par un mot de passe ou un certificat. Si le client est reconnu par le serveur RADIUS, l'AP débloque l'accès pour le client.

WPA

Le protocole *WiFi Protocted Access* WPA est une solution intermédiaire jusqu'à la finalisation de la norme 802.11i. En effet, WPA est un sous-ensemble de la norme 802.11i. Les améliorations par rapport à WEP sont :

- Authentification à l'aide de 802.1X. Pour les réseaux simples, comme ceux des utilisateurs privés, une variante appelée « Pre-shared keys » évite l'utilisation d'un serveur RADIUS. Chaque utilisateur doit alors s'authentifier auprès de l'AP à l'aide d'un mot de passe.
- Corrige les failles de sécurité de WEP. WPA utilise un nouveau protocole de cryptage, TKIP (*Temporal Key Integrity Protocol*), qui génère une clé WEP de 128 bits par utilisateur et par session. Le vecteur d'initialisation de WPA a une longueur de 48 bits au lieu de 24 bits dans WEP. Afin d'éviter toute attaque basée sur un IV connu, l'IV et la clé WEP ne sont pas simplement concaténés mais mélangés par une fonction complexe.
- Facilite la distribution des clés. Dans WEP, la clé secrète partagée devait être configurée manuellement sur chaque client. Dans WPA, une clé de sessions est générée automatiquement si l'authentification réussit.

- L'intégrité des données est assurée par un code MIC (*Message Integrity Code*, aussi appelé *Michael*) au lieu d'un code CRC. Grâce à MIC, toute modification d'un message par un intrus est détectée par le destinataire du message.

802.11i

La norme 802.11i, aussi appelée WPA2, est le pas final vers la sécurité WLAN. Elle a été finalisée en juin 2004 et les constructeurs d'équipements WLAN ont commencé l'implémentation de cette norme. La différence principale entre WPA et WPA2 est que WPA2 utilise la méthode de cryptage AES au lieu de TKIP. Ainsi le chiffrement est conforme à la législation dans certains pays (notamment les Etats-Unis) qui requiert AES pour certaines applications (gouvernement, etc.). L'inconvénient de cette solution est qu'AES est un algorithme plus complexe que TKIP (basé sur RC4). Un équipement WPA ne pourra typiquement pas être migré à WPA2 par une mise à jour du logiciel, mais nécessitera un support hardware plus performant.

Résumé

Les différentes solutions de sécurité peuvent être résumées comme suivant :

- WEP : faible !
- WEP+: WEP - IV faibles
- 802.1X : WEP + authentification RADIUS
- WPA : WEP + TKIP + 802.1X + MIC
- WPA2 : WPA + AES

Concernant l'utilisation, les conseils suivants aide à sécuriser un réseau WLAN :

- A la maison :
    - Utiliser WEP. Malgré les faiblesses, il fournit un certain niveau de sécurité
    - Utilser WPA ou WPA2 si disponible, avec authentification par mot de passe partagé (Pre-shared key)
- Dans l'entreprise
    - Utiliser WPA ou WPA2 avec un serveur d'authentification RADIUS si disponible, sinon
    - Considérer le WLAN comme un réseau externe.
        - Utiliser un logiciel de type VPN dans le WLAN.
        - Protéger le réseau interne par un firewall.

7.2.12 L'alphabet 802.11

La Table 19 résume les différents groupes de travaille du projet 802.11.

Table 19: Résumé des groupes de travail IEEE 802.11

Groupe	Objectif	Commentaire
802.11a	Couche physique pour la transmission à 54 Mb/s dans la bande de 5 GHz.	Norme achevée en 1999. Équipements pas encore disponibles.
802.11b	Couche physique pour la transmission à 11 Mb/s dans la bande de 2,4 GHz.	Norme achevée en 1999. Équipements disponibles depuis 2001.
802.11d	Adaptation de la couche MAC 802.11 à la législation dans des pays autres que les États-Unis.	Voir 802.11h pour l'utilisation de 802.11a en Europe
802.11e	Qualité de service dans les réseaux 802.11a, 802.11b et 802.11g	Norme achevée fin 2002.
802.11f	Recommandations concernant l'interopérabilité dans un environnement multi-opérateurs.	
802.11g	Couche physique pour la transmission jusqu'à 54 Mb/s dans les bandes de 2,4 GHz et de 5 GHz.	Norme attendue pour 2003
802.11h	Adaptation de la couche MAC pour l'utilisation dans la bande de 5 GHz en Europe (contrôle de puissance d'émission et sélection dynamique des fréquences)	Norme attendue pour 2003
802.11i	Améliorations de la sécurité pour les technologies 802.11a, 802.11b, 802.11g	Norme attendue pour 2003

7.3 HiperLAN

HiperLAN est la technologie WLAN prévue pour les pays européens. Il existe deux versions :

- HiperLAN 1 définie en 1998. Dans cette première version, les communications peuvent se faire sur 5 canaux distincts de priorité différente. L'adaptation du CSMA/CD appelée EY-NPMA (*Elimination Yield None Preemptive Priority Multiple Access*) consiste à scruter les canaux par ordre de priorité jusqu'à trouver un canal libre pour émettre.
  Le niveau 2 du modèle OSI est divisée en deux sous-couches, la sous-couche CAC (Channel Access Control) qui correspond à la partie physique de la technique d'accès (gestion des problèmes liés au canal hertzien ainsi que toute la transmission et réception) et la sous-couche MAC qui correspond à la partie logique, soit la mise en forme de la trame, le routage interne, les algorithmes de confidentialité, la gestion de priorité (QoS) et l'insertion et le retrait des stations.
- HiperLAN 2 est soutenu par l'H2GF (HyperLAN 2 Global Forum) fondé en 1999 par Bosch, Dell, Ericsson, Nokia, Telia et Texas Instrument. Les géants Cisco, Intel, Lucent ou Nortel sont absents de ce forum et quelques-uns des fondateurs de l'H2GF (notamment Ericsson) s'orientent actuellement plutôt vers la technologie 802.11a. Les fonctionnalités offertes par HiperLAN 2 sont les suivantes :

- **Haut débit** : la couche physique peut transmettre et recevoir des données à 54 Mb/s grâce à la modulation OFDM : *Orthogonal Frequency Digital Multiplexing*, similaire à 802.11a
- **Mode orienté-connexion** : avant chaque envoi, une connexion est établie entre les MT (terminaux mobiles) et l'AP (point d'accès). Les communications point à point sont bidirectionnelles et les communications point à multipoint sont unidirectionnelles. Un canal de broadcast permet de joindre tous les terminaux en même temps.
- **QoS** : du fait que les communications sont en mode connecté, la QoS peut facilement être implémentée. La QoS et le haut débit offrent la possibilité de faire transiter tous types de données, de la vidéo aux données.
- **Sécurité** : la norme supporte l'authentification et le chiffrement des données selon les techniques DES (56 bits) ou 3-DES.
- **Allocation automatique de fréquence** : les canaux radio utilisés sont automatiquement choisis par le point d'accès en fonction des interférences dans l'environnement et des fréquences utilisées par les autres cellules radio qui l'entourent.
- **Mobilité** : la station reçoit ces données du point d'accès le mieux situé par rapport à lui, c'est-à-dire dont le signal radio est le plus intelligible. Le changement de cellule (*roaming*) se fait automatiquement.

Bien que la conception de HiperLAN 2 semble supérieure aux normes Wi-Fi, ces dernières ont l'avantage d'être déjà disponible sur le marché. L'acceptation d'une deuxième technologie WLAN purement européenne est faible, vus aussi les efforts du groupe 802.11h qui vise une adaptation des technologies Wi-Fi aux législations européennes.

8 WirelessMAN

Du fait de la déréglementation du secteur des télécommunications dans de nombreux pays, les opérateurs téléphoniques bien ancrés dans le paysage national sont confrontés à une concurrence qui est maintenant souvent en droit de proposer des services locaux de transport de la voix et d'accès à l'internet à haut débit. Et la demande ne manque pas. Le problème pour ces nouveaux acteurs est qu'il est excessivement coûteux d'apporter une liaison par fibre optique, par câble coaxial ou même par paires torsadées de catégorie 5 à des millions d'entreprises et de particuliers.

La solution dont ils disposent est le sans-fil à large bande (*broadband wireless*). Placer une grosse antenne sur une colline aux abords d'une ville et diriger vers elle les antennes installées sur le toit de leurs clients est bien plus aisé et économique que de creuser des tranchées et de tirer des câbles. Par conséquent, ils ont tout intérêt à fournir un service de télécommunication multimégabit sans fil pour la voix, l'internet, la vidéo à la demande, etc.

La technologie LMDS (ou WLL, *Wireless Local Loop*) a justement été développée pour cela. Toutefois, il y a peu encore, chaque opérateur devait concevoir son propre

système, en raison de l'absence de standard. Cette situation empêchait la production en masse de matériel et de logiciels, ce qui favorisait des prix élevés et freinait l'acceptation.

Après que de nombreux acteurs de l'industrie eurent réalisé que la pièce manquante était une norme de réseau sans fil à large bande, un comité IEEE fut formé, composé de personnes issues d'entreprises et d'universités jouant un rôle clé. Ce comité hérita du numéro suivant disponible dans l'espace de numérotation 802, c'est-à-dire 802.16. Son travail débuta en juillet 1999 et aboutit en avril 2002 à l'approbation d'une norme portant officiellement le nom de « Air Interface for Fixed Broadband Wireless Access Systems » (interface aérienne pour systèmes d'accès fixes sans fil à large bande). Certains lui préfèrent cependant l'appellation MAN sans fil ou WMAN (WirelessMAN). Similaire à l'organisation de certification Wi-Fi pour le WLAN, un forum WiMAX a été crée par l'industrie dans le but de promouvoir cette technologie et de certifier la compatibilité et l'interopérabilité des produits de différents constructeurs.

8.1 Comparaison de 802.11 et 802.16

Quel était l'intérêt d'établir une nouvelle norme, alors qu'on disposait de la norme 802.11 ? En fait, 802.11 et 802.16 apportent des solutions à des problèmes différents.

Les normes 802.11 et 802.16 sont comparables sur certains points. En premier lieu, elles ont été élaborées pour permettre des communications sans fil à haut débit. Mais elles présentent aussi des différences significatives. 802.16 dessert des immeubles qui, par définition, ne sont pas mobiles ; ils ne changent pas de cellule. 802.11 a trait essentiellement à la mobilité. À noter aussi que les propriétaires d'immeubles sont généralement disposés à dépenser beaucoup plus pour les équipements de communication que ne le sont les propriétaires d'ordinateurs portables. Les dispositifs radio 802.16 sont donc plus perfectionnés, capables notamment de gérer des transmissions duplex. 802.11 privilégie au contraire le faible coût des équipements radio.

En outre, comme 802.16 couvre une partie d'une ville, les distances à parcourir peuvent atteindre plusieurs kilomètres. La puissance du signal radio perçue par la station de base peut donc varier considérablement. Cette variation affecte le rapport signal/bruit, et impose l'emploi de plusieurs techniques de modulation. Par ailleurs, les communications se déroulant « à l'air libre » dans une ville, il est crucial que leur sécurité et leur confidentialité soient assurées.

De plus, chaque cellule 802.16 doit pouvoir accueillir un nombre d'utilisateurs beaucoup plus grand qu'une cellule 802.11 typique, et leur offrir une bande passante bien supérieure. Effectivement, il est rare qu'une société réunisse 50 de ses employés dans une salle et les invite à visionner un film différent sur leur ordinateur portable respectif pour voir s'ils peuvent saturer le réseau sans fil 802.11. 802.16 a donc besoin d'un spectre plus étendu que celui offert par la bande des 2,4 GHz, ce qui l'oblige à opérer dans une plage de fréquences beaucoup plus hautes, qui correspondes à des ondes millimétriques.

Mais ces ondes millimétriques n'ont pas les mêmes propriétés physiques que les ondes plus longues de la bande des 2,4 GHz et requièrent, par conséquent, une couche physique complètement différente. Elles sont notamment facilement absorbées par

l'eau, en particulier par la pluie, et dans une certaine mesure par la neige, la grêle, voire par un brouillard épais. La gestion d'erreurs joue donc un rôle plus important qu'en intérieur. Elles peuvent aussi être concentrées en faisceaux directionnels, à la différence des ondes 802.11, qui sont omnidirectionnelles. Ainsi, les décisions qui ont été prises pour 802.11 relativement à la propagation multitrajet sont sans intérêt pratique pour 802.16.

Ces deux normes divergent aussi sur le plan de la qualité de service. Même si 802.11 peut gérer ponctuellement un trafic en temps réel grâce au mode PCF, elle West pas réellement adaptée à un usage téléphonique, ou intensif comme le multimédia. Au contraire, 802.16 gère parfaitement ces applications, car elle vise aussi bien les particuliers que les entreprises.

Ces différences importantes justifient l'existence de deux normes bien distinctes: 802.11 est un réseau LAN mobile, alors que 802.16 couvre un réseau beaucoup plus important, avec des utilisateurs principalement fixes.

Un MAN sans fil est beaucoup plus gourmand en ressources qu'un réseau de LAN, d'où la nécessité de disposer d'un système entièrement différent. Ceci dit, on peut se demander si 802.16 pourra servir dans le futur à la communication entre équipements portables. La norme n'a pas été optimisée à cet effet, mais cette possibilité n'est pas exclue. Pour le moment, l'accent est mis sur le sans-fil fixe.

En résumé, WirelessMAN servira principalement d'alternatif à ADLS ou cablemodem, donc comme technologie d'accès à large bande. L'utilisation principale sera par des utilisateurs fixes ou nomadiques et, possiblement dans l'avenir, mobiles.

La Table 20 résume les différences entre 802.11 et 802.16

Table 20: Comparaison entre 802.11 et 802.16

	802.11	**802.16**
Utilisation principale	Ordinateurs mobiles	Ordinateurs fixes ou nomadiques
Portée	< 100 m	Typiquement 3 – 10 km
Nombre d'utilisateurs	< 10	Des centaines de récepteurs, avec un nombre illimité d'utilisateurs
Débit	Jusqu'à 54 Mb/s	Jusqu'à 75 Mb/s
Support de QoS	Dans l'avenir (802.11e)	QoS intégrée dans la couche MAC. Approprié pour la transmission multimédia
Prix d'un récepteur	< CHF 100	Estimé à $350 en 2005 et à $100 en 2006

8.2 Les normes WirelessMAN

L'IEEE a défini trois normes, adaptées à des scénarios d'utilisation différentes : 802.16, 802.16a et 802.16e. Leurs caractéristiques sont résumées dans la Table 21

Table 21: Les différentes normes WirelessMAN

	802.16	802.16a	802.16e
Approbation	Déc. 2001	Janv. 2003	Attendue pour 2005
Fréquences	10 – 66 GHz	2 – 11 GHz	2 – 6 GHz
Transmission	Visibilité directe (Line-of-Sight)	Sans visibilité directe (Non-Line-of-Sight)	Sans visibilité directe (Non-Line-of-Sight)
Débits	32 – 134 Mb/s dans un canal de 28 MHz	Jusqu'à 75 Mb/s dans un canal de 20 MHz	Jusqu'à 15 Mb/s dans un canal de 5 MHz
Portée typique	2 – 5 km	7 – 10 km (max. 70 km)	2 – 5 km
Utilisation	Fixe	Fixe	Mobile

La norme 802.16 a été principalement prévue pour des liaisons point-à-points, similaires aux faisceaux hertziens. Le grand inconvénient est la nécessité d'une visibilité directe entre l'émetteur et le récepteur. Un autre inconvénient est la perturbation de la transmission par la pluie, la neige ou le brouillard.

La norme 802.16a est beaucoup plus intéressant comme technologie d'accès comme elle ne requiert pas de visibilité directe entre l'émetteur et le récepteur.

La norme 802.11e finalement est prévue pour des utilisateurs mobiles.