

# Réseaux locaux

*Ahmed ELLEUCH*

***Important : ce document doit être complété par les notes du cours***



## **TABLE DES MATIERES**

<b>I. Introduction .....</b>	<b>1</b>
<b>I.1 Présentation du cours .....</b>	<b>1</b>
<b>I.2 Rappels.....</b>	<b>1</b>
I.2.1 Caractéristiques des réseaux .....	1
I.2.2 Classification des réseaux .....	2
<b>I.3 Spécificités d'un LAN .....</b>	<b>3</b>
<b>II. Principes et fondements des réseaux locaux .....</b>	<b>4</b>
<b>II.1 Topologies des réseaux locaux .....</b>	<b>4</b>
II.1.1 Topologie en étoile .....	4
II.1.2 Topologie en anneau.....	5
II.1.3 Topologie en bus .....	5
II.1.4 Cas des réseaux locaux sans fils .....	6
<b>II.2 Le support physique .....</b>	<b>8</b>
II.2.1 Les paires torsadées .....	8
II.2.2 Le câble coaxial .....	9
II.2.3 La fibre optique .....	9
II.2.4 La transmission sans fils.....	11
II.2.5 Le raccordement à un câble .....	11
<b>II.3 Le mode de transmission .....</b>	<b>13</b>
<b>II.4 Les protocoles d'accès.....</b>	<b>16</b>
II.4.1 Accès par invitation à émettre ("polling") .....	17
II.4.2 Les techniques à jeton .....	17
II.4.3 Technique de la tranche vide ou anneau en tranches ("empty slot" ou "slotted ring") .....	22
II.4.4 Les techniques à accès aléatoire .....	23
II.4.5 Classification .....	28
II.4.6 Comparaison .....	29
<b>II.5 Exercices .....</b>	<b>30</b>
<b>III. Normalisation des réseaux locaux .....</b>	<b>33</b>
<b>III.1 Les normes IEEE 802.....</b>	<b>33</b>
III.1.1 Adressage MAC .....	34
III.1.2 La norme IEEE 802.2 .....	35
<b>III.2 Les normes IEEE 802.3.....</b>	<b>37</b>
III.2.1 Méthode d'accès.....	37
III.2.2 Format d'une trame .....	39
III.2.3 Primitives de service .....	39
III.2.4 Principales caractéristiques physiques .....	39
III.2.5 Evolutions de l'Ethernet vers le haut débit .....	39
<b>III.3 Les normes IEEE 802.11.....</b>	<b>41</b>
III.3.1 Méthode d'accès.....	41
III.3.2 Autres fonctionnalités (vs. réseaux filaires).....	43
III.3.3 Format d'une trame .....	47
III.3.4 Primitives de services .....	49
III.3.5 Principales caractéristiques physiques .....	49

<b>IV. Déploiement des réseaux locaux.....</b>	<b>52</b>
<b>IV.1 Ethernet.....</b>	<b>52</b>
IV.1.1 Ethernet II (DIX) vs Ethernet IEEE 802.3 .....	52
IV.1.2 Composants d'un réseau Ethernet 802.3 .....	52
IV.1.3 Composition d'un réseau Ethernet multi-segments .....	60
<b>IV.2 WiFi .....</b>	<b>64</b>
IV.2.1 Composants d'un réseau WiFi .....	64
IV.2.2 Couverture et débit.....	67
<b>IV.3 Plan de câblage .....</b>	<b>68</b>
IV.3.1 Câblage départemental .....	69
IV.3.2 Câblage d'établissement .....	71
IV.3.3 Validation du câblage .....	71
<b>V. Interconnexion des réseaux locaux .....</b>	<b>73</b>
<b>V.1 Les répéteurs .....</b>	<b>74</b>
V.1.1 Définition .....	74
V.1.2 Propriétés.....	74
<b>V.2 Les ponts .....</b>	<b>74</b>
V.2.1 Définition .....	74
V.2.2 Propriétés.....	75
V.2.3 Algorithmes de filtrage.....	75
V.2.4 Relayage des trames à travers les points d'accès .....	83
V.2.5 Translation de trames .....	85
<b>V.3 Les routeurs.....</b>	<b>88</b>
<b>V.4 Les pont_routeurs .....</b>	<b>89</b>
<b>V.5 Exercices .....</b>	<b>89</b>
<b>VI. Les réseaux sous TCP/IP .....</b>	<b>90</b>
<b>VI.1 Architecture des protocoles .....</b>	<b>92</b>
<b>VI.2 Le protocole IP (RFC 791).....</b>	<b>92</b>
<b>VI.3 Adressage (RFC990) .....</b>	<b>93</b>
<b>VI.4 Format d'un datagramme IP (RFC 791) .....</b>	<b>94</b>
<b>VI.5 Le routage IP .....</b>	<b>96</b>
<b>VI.6 Le protocole ICMP (RFC 792).....</b>	<b>97</b>
<b>VI.7 Le protocole ARP ("Address Resolution Protocol", RFC 826) .....</b>	<b>98</b>
<b>VI.8 Les protocoles du niveau transport .....</b>	<b>98</b>
VI.8.1 Les ports.....	98
VI.8.2 Le protocole UDP (RFC 768) .....	98
VI.8.3 Le protocole TCP (RFC 793).....	98
<b>VI.9 Le service DNS.....</b>	<b>100</b>
<b>VI.10 Les sockets - programmation d'une application client/serveur.....</b>	<b>101</b>
<b>VI.11 Appel de procédure à distance .....</b>	<b>106</b>
<b>VI.12 Les services de niveau supérieur .....</b>	<b>106</b>

<b>VI.13</b>	<b>Exercices.....</b>	<b>106</b>
<b>VI.14</b>	<b>Références .....</b>	<b>109</b>

# I. Introduction

Depuis les années 70 l'usage des ordinateurs s'est répandu et particulièrement, à partir des années 80, celui des micro-ordinateurs. Il était devenu courant qu'au sein d'une même entreprise les bureaux et les ateliers soient équipés d'ordinateurs qui, cependant, sont utilisés de façon séparée. D'où :

- une impossibilité de partager les ressources,
- une sous utilisation des capacités de traitement,
- une difficulté à faire communiquer différents intervenants dans une même entreprise.

Devant cet état de fait, la solution a été de chercher à relier les ordinateurs par un réseau de transmission propre à l'entreprise.

Définition d'un réseau local (LAN : "Local Area Network") : c'est un réseau informatique privé reliant des équipements informatiques situés dans un même bâtiment ou dans des **sites géographiquement proches** (exemple : campus).

## I.1 Présentation du cours

Ce cours est une initiation à la technologie des réseaux locaux, en particulier, il s'agit de :

- connaître les spécificités des réseaux locaux,
- bien assimiler les techniques d'accès à un support de transmission partagé,
- étudier l'architecture et la normalisation des réseaux locaux,
- étudier l'interconnexion au niveau 2 et l'évolution des réseaux locaux vers des réseaux commutés,
- se familiariser avec les composants matériels et le câblage des réseaux locaux
- déployer un réseau IP et configurer les services de base et
- acquérir une expérience pratique à travers des TPs ciblés.

## I.2 Rappels

### I.2.1 Caractéristiques des réseaux

Un réseau de communication est constitué d'un ensemble d'équipements ou nœuds émetteurs / récepteurs reliés par des liaisons de communication.

Un réseau se caractérise par :

- la nature des nœuds sources / destinations (téléphone, télécopieurs, ordinateurs, terminaux, commutateurs, imprimantes ...)

- la répartition géographique des nœuds à connecter (réseau interne à une machine, réseau local, régional, national ou international) ;
- le caractère public ou privé ;
- la topologie (réseau maillé, en boucle ...) ;
- les supports de transmission (supports métalliques, fibres optiques, ondes radioélectriques ...) ;
- les techniques et les protocoles de transmission ;
- le débit de transmission ;
- ...

### **I.2.2 Classification des réseaux**

Suivant la taille géographique, on distingue 4 classes de réseaux :

- i) *Les réseaux personnels (PAN : Personal Area Network)* s'étendent sur quelques mètres. Ces réseaux sont utilisés pour assurer la connectivité entre les PC, les téléphones portables, les imprimantes ainsi que d'autres terminaux... Les bus les plus couramment utilisés sont l'USB et le FireWire. Parmi les technologies sans fil on peut citer le Bluetooth, ZigBee et l'infra rouge. Selon les réseaux et les versions de ces réseaux les débits peuvent varier de quelques dizaines/centaines de Kb/s (ZigBee) à quelques Gb/s (USB 3.0, FireWire 800) avec des besoins en ressource notamment mémoire inversement proportionnel au débit : de quelques Ko (ZigBee) à quelques centaines de Ko (Bluetooth). De même l'autonomie de la batterie augmente pour les protocoles sans fils avec un moindre débit : de l'ordre de l'année pour le ZigBee et de l'ordre du mois pour le Bluetooth.
- ii) *Les réseaux locaux (LAN : "Local Area Network")* s'étendent jusqu'à quelques kilomètres et supportent des débits de l'ordre de 1 Mb/s et plus couramment aujourd'hui ils atteignent des débits de 100 Mb/s et de 1 Gb/s. Parmi les réseaux locaux, on distingue les réseaux départementaux (DAN : Departmental Area Network) et les réseaux d'établissement.

Un réseau DAN, appelé aussi réseau capillaire, a pour objectif de relier les équipements d'un même département situé souvent dans un même étage.

Un réseau d'établissement relie des réseaux DAN. Il peut être confiné dans un seul bâtiment (BAN : "Building Area Network") ou desservir plusieurs bâtiments géographiquement très proches (CAN : "Campus Area Network").

Un Réseau local d'Entreprise (RLE) est un réseau utilisée pour la bureautique. Un Réseau Local Industriels (RLI) est spécifique au monde industriel et pour lequel les équipements connectés peuvent être, en plus des équipements informatiques, des

robots, des machines outils, des capteurs ... Les contraintes dans un RLI sont plus sévères particulièrement en termes de disponibilité et de garanti de temps d'accès.

iii) *Les réseaux métropolitains (MAN : "Metropolitan Area Network")*. Une extension des réseaux locaux est celle où les bâtiments, d'une même entreprise, peuvent être distants de plusieurs dizaines de kilomètres dans une même métropole (< 100 Km) et reliés par un réseau haut débit dit réseau MAN. Pour un tel réseau, les communications distantes se font par l'intermédiaire d'une infrastructure publique de télécommunication ("carrier").

iv) *Les réseaux étendus (WAN : "Wide Area Network")*

- à faible et moyen débit (< 100 Kb/s) : réseaux téléphoniques, réseaux télex, d'anciens réseaux de transmission de données (X.25, réseaux constructeurs : SNA, DNA,...),

- à haut débit (> 1 Mb/s) : réseaux satellites, réseaux câblo-opérateurs, RNIS, FR, ATM ...).

### **I.3 Spécificités d'un LAN**

De part la définition d'un réseau local on peut dégager les caractéristiques suivantes :

i) un étendu géographique limité ;

ii) le caractère privé à un organisme ou une entreprise ;

iii) la possibilité d'interconnecter des équipements variés provenant de différents constructeurs (ordinateurs, terminaux, périphériques ...).

De plus, étant donné les contraintes d'utilisation, se rajoutent d'autres caractéristiques parmi lesquels on peut citer :

iv) un débit élevé supérieur au Mégabit par seconde ;

v) un temps de réponse faible de l'ordre de la centaine de microseconde ;

vi) un taux d'erreur faible (<  $10^{-9}$ ) ;

vii) une stabilité en pleine charge ;

viii) la facilité d'extension, de reconfiguration et de maintenance.

Notons que les réseaux locaux industriels sont utilisés pour interconnecter divers équipements de contrôle et de mesure, ils nécessitent des contraintes plus sévères quant à la fiabilité (tolérance aux pannes) et le comportement déterministe, en particuliers, les temps de transmission doivent être bornés.



## **II. Principes et fondements des réseaux locaux**

Un réseau local se caractérise notamment par :

- sa topologie,
- le support de transmission,
- le mode de transmission et
- la méthode d'accès.

### **II.1 Topologies des réseaux locaux**

La topologie d'un réseau décrit la configuration physique relative à l'interconnexion des nœuds entre eux au moyen d'un support de transmission. Différentes topologies, illustrées par la figure 1, sont décrites dans ce qui suit. Notons que nous pouvons distinguer deux types de liaison :

- une liaison point à point reliant deux nœuds,
- une liaison multipoint partagée par plusieurs nœuds.

#### Remarque :

La mise en œuvre d'un réseau local se situe au niveau des couches physique et liaison du modèle de référence. Indépendamment du type de liaisons utilisées (point-à-point ou multipoint), un réseau local est généralement considéré comme une "liaison" multipoint.

#### **II.1.1 Topologie en étoile**

La topologie en étoile est composée d'un nœud de commutation central auquel sont reliés, par des liaisons point à point, tous les autres nœuds. D'une manière générale, la commutation est soit une commutation de circuits soit une commutation de trames/paquets. Dans le cas des réseaux locaux, il s'agit d'une commutation de trames.

#### Avantages :

- facilité d'extension dans la limite du nombre de ports ;
- facilité de maintenance ;
- facilité de détection de panne ;
- la défaillance d'un nœud, autre que le nœud central, ne paralyse pas les communications sur le réseau ;
- possibilité de réaliser plusieurs communications en parallèle à travers la commutation tout en construisant des commutateurs rapides, à haut débit avec un délai de traversée de l'ordre de quelques dizaines de microsecondes.

#### Inconvénients :

- le risque de surcharge du nœud central ;

- la défaillance du nœud central paralyse toute communication à travers le réseau ;
- l'extensibilité du réseau est limitée ; Afin de remédier à cette limite Une autre extension possible de la topologie en étoile est celle où plusieurs commutateurs sont reliés au moyen de répéteurs pour former un réseau dit en arbre.
- la diffusion peut nécessiter des mécanismes / opérations particulières ;
- longueur totale du câblage importante.

### **II.1.2 Topologie en anneau**

Dans une topologie en anneau, les nœuds sont reliés entre eux par des liaisons point-à-point, l'ensemble forme une boucle. Les messages transitent de nœud en nœud suivant un sens de rotation. Le câblage d'un réseau local en anneau est le plus souvent en étoile.

#### Avantages :

- simplicité de l'acheminement des messages ;
- le signal reste toujours de bonne qualité car il est régénéré à chaque passage par un nœud ;
- extension relativement facile ;

#### Inconvénients :

- à défaut de mécanismes supplémentaires,
  - ~la défaillance d'un nœud ou d'une liaison paralyse le réseau ;
  - ~l'ajout ou la suppression d'un nœud nécessite l'interruption du fonctionnement normal du réseau ;
- coûteuse puisqu'il est nécessaire d'assurer la répétition du signal, la synchronisation entre toute paire de voisin, la réduction des temps de latence sur chaque station intermédiaire ...

### **II.1.3 Topologie en bus**

Dans le cas d'une topologie en bus tous les nœuds sont raccordés à une même liaison physique multipoint appelée bus. Dans le cas des réseaux locaux, le contrôle d'accès est soit centralisé au niveau d'un nœud maître, soit réparti à travers les différents nœuds. Il est possible d'étendre la longueur physique d'un bus au moyen de répéteurs. Dans le cas des réseaux locaux, la tendance a été de remplacer le bus par un nœud central appelé HUB. Ce dernier envoie un signal reçu à travers une entrée sur toutes les sorties. La topologie physique est ainsi ramenée à une étoile. Le fonctionnement reste comparable à celui d'un bus.

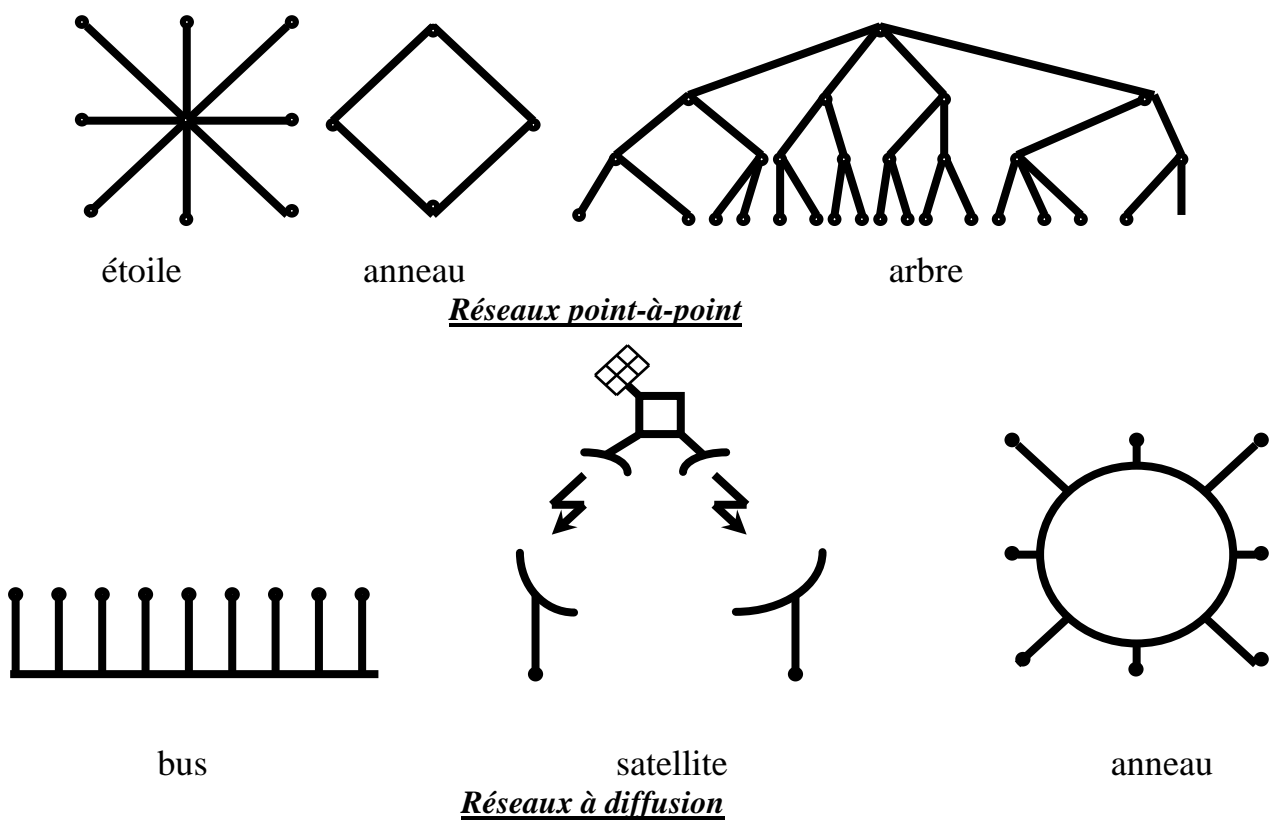
#### Avantages :

- facilité d'ajout ou de suppression d'un nœud ;
- la défaillance d'un nœud n'a presque pas d'incidence sur le réseau (sauf s'il se met à émettre sans respecter les règles d'accès) ;

- propriété de diffusion (suite à une même émission) ;
- coût relativement faible (câblage).

Inconvénients :

- une coupure du réseau divise le réseau en deux et rend le réseau non opérationnel ;
- Le délai de propagation d'un signal sur le bus augmente avec la longueur du bus. Afin de d'augmenter les possibilités d'extension sans augmenter ce délai, il est possible de relier plusieurs bus au moyen de répéteurs suivant une structure arborescente.
- un seul nœud peut émettre à la fois (dans le cas d'une transmission symétrique).



*Figure 1 : les différentes topologies en point à point et en diffusion*

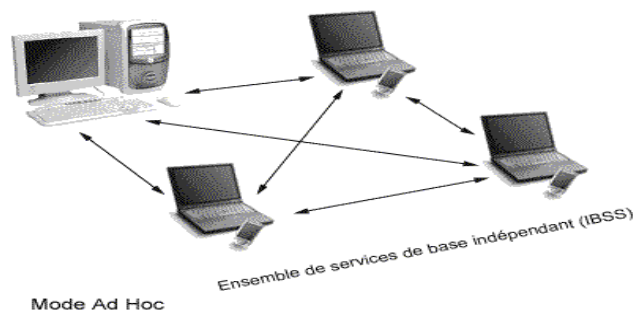
#### **II.1.4 Cas des réseaux locaux sans fils**

Il existe deux modes de fonctionnement dans le cas des réseaux locaux sans fils :

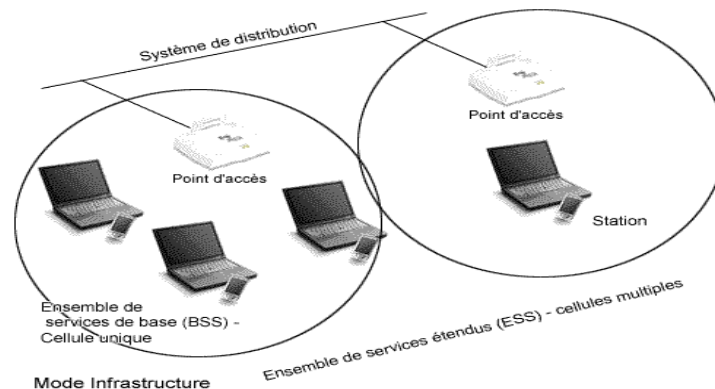
- Le mode Ad-Hoc (IBSS: "Independent Basic Service Sets") : ce mode permet de connecter directement les ordinateurs (figure 2-a), sans recourir à un équipement tiers. Ce mode est approprié pour échanger des fichiers entre portables dans un lieu quelconque (café, train ...). La mise en place d'un tel réseau se ramène à sélectionner un canal (fréquence) et un nom de réseau (SSID) communs à tous. Grâce à l'ajout d'un logiciel de routage dynamique (OLSR : "Optimized Link State Routing", AODV : "Adhoc On Demand

Distance Vector" ...), il est possible de créer des réseaux maillés autonomes dans lesquels la portée ne se limite pas aux voisins.

- Le mode infrastructure (BSS: "Basic Service Set" ou ESS: "Extended Service Set") : ce mode de fonctionnement permet de connecter les ordinateurs entre eux à travers un ou plusieurs équipements intermédiaires qui concentrent le trafic et appelés Points d'Accès ou AP (figure 2-b). Ce mode est essentiellement utilisé comme extension de réseaux filaires. Les APs ainsi que les ordinateurs, doivent être configurés avec le même nom de réseau afin de pouvoir communiquer. Il est donc possible de déterminer les nœuds connectés au réseau.



*Figure 2-a: Mode Ad-Hoc (IBSS)*



*Figure 2-b : Mode Infrastructure (BSS+ESS)*

Avantages :

- la mobilité ;
- la facilité d'ajout ou de suppression d'un nœud ;
- la défaillance d'un nœud, mis à part l'AP en mode infrastructure, n'a presque pas d'incidence sur le réseau ;

Inconvénients :

- en mode infrastructure, la défaillance d'un AP rend non opérationnelle la cellule correspondante ;
- taux d'erreurs, sensibilité aux bruits et aux obstacles,
- la diffusion ne permet pas de joindre forcément toutes les stations,

- un seul nœud peut émettre à la fois (dans le cas d'un seul canal),
- problèmes de sécurité : besoin de recourir à des techniques d'authentification et de cryptage ;

## **II.2 Le support physique**

Du choix du support physique dépendent les performances du réseau notamment le débit de transmission ainsi que la fiabilité du réseau. La plus part des réseaux locaux utilisent un signal électrique véhiculé sur des supports métalliques. On trouve aussi, de plus en plus, des réseaux à fibres optiques permettant des débits plus élevés et une meilleure fiabilité. Par ailleurs, la transmission peut s'effectuer sans que les signaux ne soient guidés par un support : onde radio électromagnétique, rayons infrarouges, rayons laser ...

Dans ce qui suit, sont décrits les supports utilisés à savoir les paires torsadées, les câbles coaxiaux et la fibre optique ainsi que les bandes de fréquence utilisées. La figure 3 représente une illustration de ces supports.

### **II.2.1 Les paires torsadées**

Le câble est constitué d'une ou plusieurs paires de fils de cuivre en spiral (en torsade). Chaque fil est recouvert d'une gaine. Plusieurs paires peuvent être regroupées dans une même gaine.

#### Caractéristiques :

- se prête bien à une liaison point à point ;
- s'utilise pour une transmission analogique ou numérique ;
- affaiblissement des signaux important suivant la longueur ;
- le débit dépend notamment du type de la liaison et de la longueur. De l'ordre du Kb/s ou moins pour une liaison multipoint ainsi que pour une liaison point à point d'une longueur supérieure au kilomètre. De quelques centaines de Kb/s jusqu'à plusieurs dizaines de Mb/s (voire même 100 Mb/s ou 1 Gb/s) lorsque la longueur est de plus en plus courte ;
- sensible aux perturbations électromagnétiques et au problème de diaphonie. La diaphonie se produit par la transmission d'un signal parasite d'une paire vers les autres paires. L'affaiblissement de ce signal (paradiaphonie) s'obtient par le torsadage et en réduisant la proximité des paires. En outre, pour réduire ces perturbations, les paires torsadées, d'un même câble, peuvent être entourées d'une tresse métallique ou pellicule ou feuille d'aluminium, le câble est dit écranté. Cette pellicule évite le couplage de rayonnements perturbateurs haute fréquence (actifs à partir de 25 Mhz environ). Différents types de blindage existent comme le montre la figure 3. Si le blindage n'est pas correctement mise à la masse, des courants parasites apparaissent et le support se comporte moins bien qu'une paire torsadée

sans blindage (qui est de surcroît moins cher). Les organismes EIA (« Electronic Industries Association ») et TIA (« Telephone Industries Association ») ont élaboré une norme EIA/TIA-568 définissant les caractéristiques minimales de différentes catégories (3, 4, 5, 6, 7) de paires torsadées notamment en ce qui concerne la bande passante et l'affaiblissement en fonction de l'impédance ; les paires torsadées de catégorie 5 sont les plus utilisées alors que les câbles blindés, introduits par IBM, n'ont pas eu un succès comparable.

- simple à installer et coût relativement faible notamment dans le cas des câbles de catégorie 3.

#### Utilisation :

- Topologies : étoile et anneau ;
- les réseaux DAN (entre le répartiteur d'étage et les nœuds de l'étage).

### **II.2.2 Le câble coaxial**

Il est constitué d'un câble central entouré d'un isolant et d'une tresse métallique, le tout enveloppé par une gaine protectrice.

#### Caractéristiques :

- se prête bien à une liaison point à point ou multipoint ;
- s'utilise pour une transmission analogique ou numérique ;
- moins simple à installer que la paire torsadée ;
- plus coûteux que la paire torsadée ;
- on distingue, notamment, deux types de câbles coaxiaux :
  - câble 50  $\Omega$  utilisé en bande de base,
  - câble 75  $\Omega$  (ou CATV : "Community Antenna TeleVision"), utilisé en large bande
- le débit dépend de la longueur du câble et de ses caractéristiques, il est de l'ordre de quelques Mb/s à plusieurs dizaines de Mb/s (sur une longueur de 1 Km ) voire même 1 Gb/s ;

#### Utilisation :

- topologies : bus, anneau, arbre ;
- tendance à le remplacer par la paire torsadée au niveau des réseaux DAN, et par la fibre optique pour le reste du câblage.

### **II.2.3 La fibre optique**

Une fibre optique se compose d'un noyau entouré d'une gaine. Le noyau est un guide cylindrique optique ayant un fort indice de réfraction dans lequel se propagent des faisceaux lumineux (ondes optiques). La gaine confine les ondes optiques. Le tout est recouvert par une ou plusieurs enveloppes de protection. Un câble en fibre optique comporte généralement plusieurs brins regroupés par multiple de 2, 6, 8 ...

Aux extrémités d'un câble se trouve l'émetteur et le récepteur. L'émetteur est composé d'un codeur et d'une Diode Electro Luminescente (DEL) ou d'une Diode Laser (DL) ou encore d'un laser modulé. Le récepteur est constitué d'un décodeur et d'un détecteur de lumière (photodétecteur). Le rayon laser a pour avantages d'être une lumière intense, monochromatique, stable en amplitude et en fréquence, avec un phénomène de dispersion faible. Les diodes laser sont plus chères et durent moins.

On distingue deux types de fibres optiques :

- la fibre monomode : un seul angle d'incidence, diamètre de quelques microns, vitesse de propagation de l'ordre de 0,25 millions de kilomètre par seconde, bande passante jusqu'à 100 Ghz/Km voire même plusieurs milliers de Ghz/Km ;
- la fibre multimode : plusieurs angles d'incidence, diamètre de quelques centaines de microns, vitesse de propagation de l'ordre de 0,1 millions de kilomètre par seconde, moins chère. Parmi les fibres multimode on distingue :
  - la fibre multimode à saut d'indice dont le noyau a un seul indice de réfraction, bande passante allant jusqu'à 50 Mhz/Km ;
  - la fibre multimode à gradient d'indice dont le noyau a un indice de réfraction qui diminue progressivement en s'éloignant de l'axe, bande passante allant jusqu'à 1 Ghz, vitesse propagation plus importante que celle pour la fibre à saut d'indice. La fibre optique multimodes à gradient d'indice semble être la meilleure solution pour les roades et les distances supérieures à 100 m. Elle est déjà largement utilisée pour fédérer les réseaux.
- bien que la largeur de la bande passante que peut atteindre un support en fibre optique est énorme, le débit est limité actuellement à quelques Gb/s, ceci est dû à l'impossibilité d'effectuer des conversions entre les signaux électriques et les signaux optiques plus rapidement.

#### Caractéristiques :

- s'utilise pour une liaison point à point, cependant il est délicat de l'utiliser pour une liaison multipoint à cause des difficultés de dérivation ;
- le plus difficile à installer (raccordement, dérivation ...) ;
- le plus coûteux ;
- bande passante et débit important ;
- pas de diaphonie, insensible aux perturbations électromagnétiques, faible atténuation, résistance à la chaleur, au froid et à l'humidité ;
- encombrement et poids inférieurs aux autres supports (<1/10).

#### Utilisation :

- topologies anneau, étoile

- tendance à utiliser la fibre optique multimode particulièrement dans les réseaux d'établissement.

#### **II.2.4 La transmission sans fils**

Les réseaux locaux sans fils utilisent des ondes radio ou infrarouges. Particulièrement, ils utilisent les bandes de fréquence (dans la gamme des micro-ondes) sans licence suivantes:

- ISM "Industrial Scientific and Medical" : 3 sous-bandes cédées en 1985 par l'armée US,
- U-NII "Unlicensed-National Information Infrastructure".

Plusieurs techniques de transmission ont été définies afin de limiter les problèmes dus aux interférences et afin d'augmenter le débit (cf. §II.3).

##### Caractéristiques :




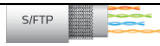
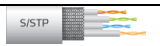
- Plus la puissance d'émission est élevée, meilleure est la couverture, mais la consommation d'énergie est plus grande.
- Plus la fréquence radio est élevée, meilleur est le débit, mais la couverture est moins bonne.
- Plus le débit est élevé, plus la couverture radio est faible.
- Les signaux se comportent différemment dans l'environnement selon leur fréquence ; dans la gamme des micro-ondes :
  - les gouttes de pluie atténuent davantage les signaux à haute fréquence,
  - les micro-ondes sont en partie réfléchies par la plupart des objets. Un signal peut être réfléchi plusieurs fois, le récepteur capte donc plusieurs signaux avec de légers décalages de temps,
  - au-delà de 5 GHz (le haut du spectre des micro-ondes), les ondes ne pénètrent quasiment plus les objets. L'émetteur et le récepteur doivent être en vue directe sans obstacle « *clear line of sight* ».

#### **II.2.5 Le raccordement à un câble**

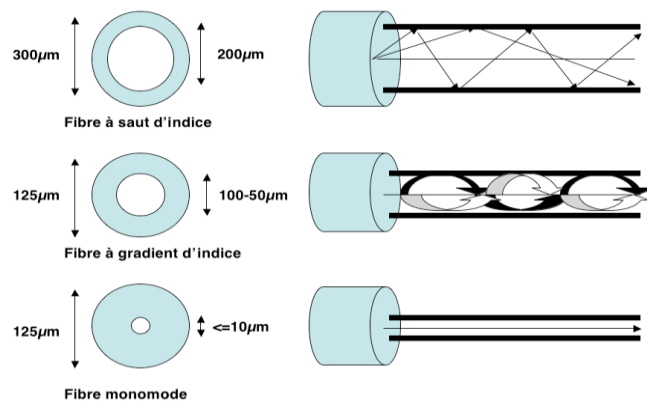
Le raccordement se fait grâce à un coupleur (carte réseau) dont la fonction est d'assurer l'accès au support de transmission. Le raccordement est décrit par la figure 4. A noter que l'adaptateur peut être intégré au coupleur.



### Paires torsadées

	Cat. 3 Classe C	Cat. 5 Classe D	Cat. 5 E	Cat. 6 Classe E	Cat. 7 Classe F	Structure	Autre dénomination
<b>Bande Pass.</b>	16 MHz	100 MHz	100 MHz	200 MHz	600 MHz	UTP 	U / UTP
<b>Type</b>	UTP	UTP/ FTP	UTP/ FTP	UTP/ FTP	SSTP	STP 	U / FTP
<b>Coût</b>	0.7	1	1.2	1.5	2.2	FTP 	F / UTP
						S/FTP 	SF / UTP (de Cat5e)
						S/SSTP 	ou S / FTP (de cat6 ou +)

### Fibres optiques



### Bandes de fréquences

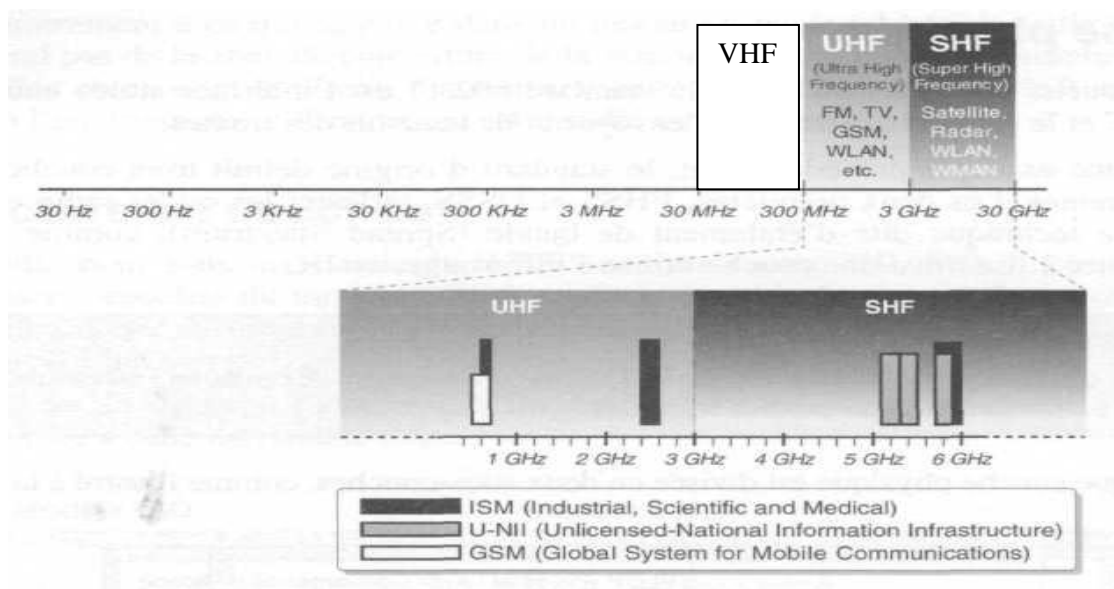
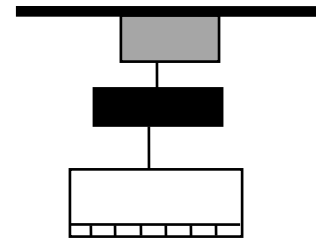


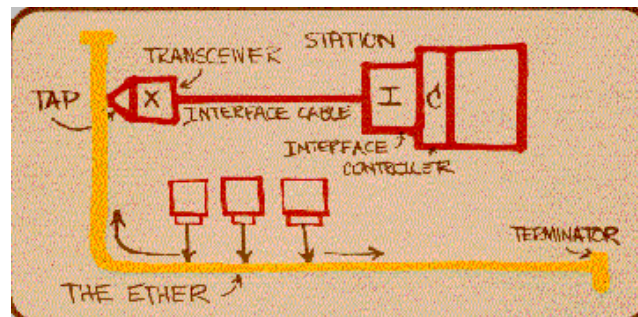
Figure 3 : les différents supports de transmission

le support physique : câble.....  
la prise (tap) : connexion mécanique.....  
l'adaptateur : modem, transceiver (codage,...)..

le coupleur : contrôle d'accès .....  
l'interface : entre l'équipement et le coupleur.



*Dessin réalisé par Robert M. Metcalfe pour présenter le concept Ethernet en 1976*



*Figure 4 : raccordement d'une station*

### II.3 Le mode de transmission

Les deux modes, en bande de base et large bande, sont utilisés. Rappelons que pour la transmission en bande de base, l'information est directement traduite par des changements discrets du signal et suivant un codage donné (exemple : code Manchester, le code Manchester différentiel, en bloc 4B/5B, 8B/10 ...). Ces codes incluent le signal d'horloge. Pour la transmission en large bande, le signal numérique est modulé sur une onde porteuse (variation de la fréquence, de l'amplitude et / ou de la phase).

Les systèmes en bande de base sont plus simples à mettre en œuvre et moins coûteux. Bien que suivant ce mode de transmission le signal tend à s'affaiblir rapidement avec la distance, l'utilisation de répéteurs permet de remédier à ce problème. Pour ces raisons, dans le cas des réseaux locaux filaires, la transmission en bande de base est la plus utilisée. En revanche, les réseaux locaux sans fils font appel à une transmission par modulation. Des techniques d'étalement de fréquences sont utilisées. A l'origine, elles étaient utilisées pour la lutte contre les brouillages dans les systèmes militaires. Au lieu de transmettre à travers un canal ayant une bande passante étroite, la transmission est effectuée à travers un large spectre de fréquences avec des signaux de plus faible puissance. En moyenne la puissance reste la même : les signaux transmis sont considérés comme du bruit par les utilisateurs qui travaillent en bande étroite. Cet élargissement du spectre rend le signal moins sensible aux perturbations

provenant de signaux en bande étroite. Parmi les techniques d'étalement de spectre nous citons :

- La technique d'étalement de spectre par saut de fréquence (**FHSS** : "Frequency Hopping Spread Spectrum"), elle consiste à découper une large bande de fréquence en canaux, puis à transmettre en utilisant une séquence aléatoire de canaux connue de toutes les stations d'une même cellule. La transmission s'effectue successivement sur un canal puis sur un autre (à chaque fois pendant une courte période, environ 300 ms) et ceci afin réduire les interférences entre les transmissions des diverses stations. Aussi, le saut de fréquence est particulièrement utile pour contrer la propagation du signal suivant des trajets multiples : le signal le "plus direct" arrive en premier, les signaux réfléchis suivent des trajets plus longs et arrivent en retard après que le récepteur ait changé de fréquences. Cependant, il est nécessaire de maintenir une synchronisation très stricte entre l'émetteur et le récepteur. Suivant la norme 802.11, la bande de fréquence est 2.4-2.483, elle permet de créer 79 canaux de 1 MHz (bande ISM), il est possible de faire fonctionner 26 réseaux dans une même zone. Le débit est limité à 2 Mb/s.
- La technique d'étalement de spectre à séquence directe (**DSSS** : "Direct Sequence Spread Spectrum") utilise la bande ISM de 83.5 Mhz, elle est divisée en 14 (Europe) canaux de 22 MHz qui se recouvrent. Pour permettre à plusieurs réseaux de couvrir une même zone, il faut allouer à chacun d'eux des canaux qui ne se recouvrent pas (donc au maximum 3 réseaux). Puisque certains canaux se recouvrent partiellement, des canaux isolés (les canaux 1, 6 et 11) distants les uns des autres de 25MHz sont généralement utilisés. Pour éviter toute interférence il est recommandé d'organiser la répartition des points d'accès et l'utilisation des canaux de telle sorte que deux points d'accès utilisant les mêmes canaux ne se recoupent pas. En comparaison avec la technique FHSS, la technique DSSS permet d'augmenter le débit. Du fait qu'un seul canal est utilisé cette technique est plus sensible aux interférences. Pour remédier à ce problème, la technique de « chipping » est utilisée, un bit est représenté par une séquence dite Barker de 11 bits. Cette séquence redondante permet d'effectuer des contrôles (et même de correction) d'erreurs. Différents débits sont possibles : 1Mb/s (code Barker, modulation de phase BPSK " Binary Phase Shift Keying"), 2 Mb/s (code Barker, modulation QPSK pour Quadrature PSK), 5,5 et 11 Mb/s (une méthode alternative appelée CCK "Complementary Code Keying" permet d'encoder directement plusieurs bits en utilisant une même 8 bits ou puces (au lieu de 11 bits). Ainsi en codant simultanément 4 bits utiles, la

méthode CCK permet d'obtenir un débit de 5.5 Mbps et elle permet d'obtenir un débit de 11 Mbps en codant 8 bits de données).

- Une autre technique de modulation est la technique OFDM (Orthogonal Frequency Division Multiplexing), elle utilise des canaux distincts, chaque canal est divisé en un grand nombre de sous-canaux (modulation multi-porteuse). Cette technique de modulation permet d'obtenir des débits élevés en envoyant les données en parallèle sur les différentes fréquences (54 Mbps pour le Wifi/IEEE 802.11a/g). L'OFDM autorise un fort recouvrement spectral entre les sous-porteuses ce qui permet d'augmenter le nombre de sous-canaux. Pour que ce recouvrement ne pose pas de problèmes d'interférence, les porteuses doivent respecter une contrainte d'orthogonalité. Ceci est réalisé en assurant un espacement régulier de  $1/T$  entre les sous-porteuses, où  $T$  est la période qui sépare 2 symboles de  $N$  données (nombre de sous-porteuses). Ainsi, lorsque le spectre d'une sous-porteuse est maximal, le spectre des sous-porteuses voisines s'annule, il est donc possible d'avoir un recouvrement entre les spectres de différentes sous-porteuses tout en évitant les interférences entre elles (l'échantillonnage doit s'effectuer précisément à la fréquence d'une sous-porteuse).
- Toutes les techniques déjà décrites utilisent une antenne de chaque côté et sont considérées comme étant SISO « Single Input Single Output », une autre alternative - dite MIMO « Multiple Input Multiple Output » - est de recourir à plusieurs antennes d'émission/réception. Différentes techniques MIMO existent. Une première technique, dite à diversité spatiale, consiste à émettre un même message sur différentes antennes : (1) les mêmes signaux mais déphasés puis sommés pour augmenter le rapport signal/bruit ou encore (2) retenir le meilleur signal parmi deux signaux, par exemple. Une deuxième technique, dite à multiplexage spatial, consiste à découper le message en plusieurs flux et envoyer ces flux à travers différentes antennes en parallèle. Une troisième technique, dite de « beamforming », consiste à combiner les antennes de telle façon à ce que les signaux interfèrent de manière constructive dans certaines directions (voulues) et destructives dans les autres directions. Par ailleurs, les techniques MIMO peuvent être « Single User » (SU-MIMO) où seul un utilisateur à la fois est en communication avec le point d'accès ou « Multiple-user » (MU-MIMO) où plusieurs utilisateurs peuvent être en communication avec le point d'accès (selon le nombre d'antennes). Il est possible que ces communications multiples soient dans un seul sens du point d'accès vers le l'utilisateur (liaison descendante) ou dans les deux sens.

- Issues de ces techniques, différentes versions des réseaux WiFi existent :

802.11	Débit max (Théorie)	Portée typique	Fréquence (Ghz)	Nombre de canaux	Largeur bande D'un canal	Modulation	MIMO
802.11 - 1997	2 Mbit/s	20 m	2,4	79/13	1/22 Mhz	FHSS, DSSS	Non
802.11a (WiFi 2) (1999)	54 Mbit/s	35 m	5	4-12	20	OFDM	Non
802.11b (WiFi 1) (1999)	11 Mbit/s	35 m	2,4	13	22	DSSS	Non
802.11g (WiFi 3) (2003)	54 Mbit/s	38 m	2,4	3/7/13	20	DSSS, OFDM	Non
802.11n (WiFi 4) (2009)	72 – 288 Mbit/s	70 m	2,4	8 4	20 40	OFDM	Oui Max 4
802.11n (WiFi 4) (2009)	150 – 600 Mbit/s	35 m	5	19 9	20 40	OFDM	Oui Max 4
802.11ac (wave 1 2013 et wave 2 2016 WiFi 5) ()	433 – (1300/wave1 2600/wave2 Mbit/s)	35 m	5	2x80Mhz 1	20, 40, 80 160 MHz	OFDM	Oui Max 8 +(MU-MIMO wave 2)
802.11ax (fin 2020)	10 Gbit/s	12-35 m	2,4 et 5		20, 40, 80 160 MHz	OFDM	Oui MU-MIMO dans les deux sens Max 8
...							

## II.4 Les protocoles d'accès

Comme pour tout système où l'on veut partager une ressource, dans un réseau local, il est nécessaire de mettre en œuvre un protocole (ou méthode) d'accès au support physique de transmission. Le partage d'un canal de communication peut s'effectuer suivants différents critères.

Classification 1 :

- accès **aléatoire** (par contention), ne nécessite pas une autorisation préalable,
- accès **déterministe** où un mécanisme permet de désigner la station (primaire) qui peut émettre.

Classification 2 :

- accès **statique** où l'allocation de la bande passante est définitive,
- accès **dynamique** (adaptatif) où l'allocation de la bande passante évolue selon les besoins.

Classification 3 :

- l'approche **centralisée** où seul un nœud primaire attribue des droits d'accès,
- l'approche **distribuée** où les différents nœuds participent de la même façon aux contrôles d'accès.

Classification 4 :

- partage **temporel** (TDMA : "Time Division Multiple Access"),
- partage **fréquentiel** (FDMA : "Frequency Division Multiple Access").

#### **II.4.1 Accès par invitation à émettre ("polling")**

Les nœuds du réseau sont interrogés successivement (suivant un certain ordre) pour déterminer à chaque fois si le nœud interrogé a un message à émettre. Pour cela, une invitation à émettre est issue d'un nœud primaire vers un nœud secondaire, si ce nœud secondaire ayant reçu cette invitation veut émettre, il répond positivement à cette invitation.

Utilisation : cette technique est utilisée dans le cas de liaisons longues distances, elle est aussi utilisée dans des réseaux de terminaux en bus. Par ailleurs elle a été retenue dans le cas des réseaux locaux Ethernet 100VG Any LAN. Appelée méthode PCF « Point Coordination Function », elle est aussi prévue dans les réseaux locaux sans fil WiFi, en mode infrastructure, pour des applications temps réels. Elle n'est pas la méthode d'accès généralement utilisée par les réseaux WiFi (elle n'est pas systématiquement implémentée). La méthode PCF assure un service sans contention durant des périodes obtenues grâce à une méthode avec contention (DCF— « Distributed Coordination Function »), cf. II.4.4.

#### **II.4.2 Les techniques à jeton**

Le principe du contrôle d'accès à l'aide d'un jeton consiste à faire circuler sur le réseau une permission d'émettre, appelée jeton ("token"), de sorte que seul le nœud qui détient le jeton a l'autorisation d'émettre un message. Le jeton peut être dans l'un des deux états : libre ou occupé. Pour qu'un nœud puisse émettre un message, il doit attendre que le jeton lui parvienne à l'état libre, auquel cas, le jeton est positionné à l'état occupé, le nœud est en mesure d'entamer son émission. Les autres nœuds voient

passer le message, le destinataire doit se reconnaître et recopier le message. Dans le cas d'une topologie en anneau, c'est l'émetteur du message qui prélève ce dernier et ensuite passe le jeton libre.

Suivant ce principe, plusieurs techniques à jeton existent. Elles diffèrent en particulier selon :

- le choix du prochain nœud qui aura la possibilité de détenir le jeton. Soit que la circulation du jeton se fait suivant l'ordre des nœuds dans un anneau physique (jeton non adressé), soit que le jeton est adressé à nœud spécifique suivant un anneau logique (particulièrement appliqué dans le cas d'une topologie en bus) ;
- l'instant de renvoi du jeton libre. Pour une topologie en anneau, ceci peut se faire lorsqu'une station, ayant émis une trame, reçoit cette trame (possibilité d'effectuer des vérifications) ou dès la réception de l'en-tête de la trame ou encore dès la fin de l'émission de la trame. Cette dernière solution permet de mieux utiliser la bande passante en ayant plusieurs trames de données, issues de différents nœuds, qui circulent en même temps sur le réseau.
- la gestion des priorités.

L'utilisation du jeton nécessite un mécanisme pour garantir la présence et l'unicité du jeton. Dans une première approche centralisée, un nœud de supervision (moniteur) est utilisé à cet effet. En cas de défaillance, le moniteur peut changer de nœud. Un délai de garde est défini au bout duquel, si le jeton ne repasse pas par le moniteur, le réseau est purgé et le jeton est re-généré par le moniteur.

Dans une seconde approche distribuée, chaque coupleur maintient un temporisateur ayant une valeur propre. Si le délai de garde d'un coupleur s'écoule sans qu'aucun message ne passe, le coupleur re-génère le jeton. Il faut aussi prévoir des mécanismes supplémentaires pour éviter que deux jetons ne soient re-générés. Ceci est aussi nécessaire dans le cas général car une séquence quelconque de bits peut se transformer en un deuxième jeton.

Les techniques de contrôle d'accès utilisant un jeton permettent de garantir une borne supérieure du temps d'accès au support physique. Cette borne peut être calculée en fonction notamment de la quantité maximale d'informations qu'il est possible d'émettre à chaque passage du jeton et le nombre de nœuds connectés au réseau.

Utilisation : le contrôle d'accès à l'aide d'un jeton est la méthode privilégiée des réseaux en anneau, elle est aussi utilisée pour la topologie en bus.

Dans ce qui suit, en se référant à d'anciennes normes utilisant la méthode des jetons, nous illustrons davantage le fonctionnement de telles méthodes

#### *II.4.2.1 Cas du jeton sur anneau*

Principales règles de fonctionnement (inspiré du "token-ring »/IEEE802.5) :

- Disposant du jeton il est possible d'émettre plusieurs trames de suite, un temporisateur (THT : « Token Holding Timer ») contrôle le temps maximum de détention du jeton (par défaut 10 ms).
  - Retrait d'une trame par son émetteur.
  - La libération du jeton se fait dès la réception de l'en-tête de la première trame.
  - Le jeton est libéré lorsque l'entête de la trame revient à l'émetteur.
  - Utilisation d'un mécanisme de priorité (description simplifiée)
    - A chaque message  $M_I$  est associée une priorité  $I$  (8 niveaux sont définis). Sur chaque nœud le message le plus prioritaire est noté  $M_S$ . Au jeton est associée une priorité courante  $P$  et une priorité  $R$  de réservation.  $P$  et  $R$  sont initialisées à la priorité la plus basse 0.
    - Un jeton libre ne peut être pris par un nœud que si  $S \geq P$  ( $S$  relative à ce nœud). Si en plus,  $P < S$  alors  $S$  est affectée à  $P$  et  $R$  est mise à 0.
    - Un nœud par lequel passe le jeton occupé ou de priorité  $P > S$  ( $S$  relative à ce nœud), met à jour  $R$  par la valeur de  $\text{Max}(R, S)$ .
    - Le jeton est libéré au retour et lorsque le nœud qui le détient ne dispose plus de message de priorité supérieure ou égale à  $\text{Max}(P, R)$  ou aussi lorsque le THT a expiré,  $R$  est mis à jour à  $\text{Max}(R, S)$ . Lors de la libération du jeton, si  $R > P$ , la valeur de  $R$  est affectée à  $P$  et  $R$  est mise à 0.
    - Tout nœud ayant augmenté la valeur de  $P$  devient une station de stockage et mémorise l'ancienne valeur de  $P$  dans une pile  $S_r$  et la nouvelle valeur de  $P$  dans une autre pile  $S_x$ . Lorsque le jeton lui revient libre, ou vient d'être libéré, avec la même nouvelle valeur (de  $S_x$ ), si la valeur de  $R$  (ayant été mise à jour localement par  $\text{Max}(R, S)$ ) est inférieure à l'ancienne valeur de  $P$ , tête de  $S_r$ , celle-ci est dépilée et affectée à  $P$  (la tête de  $S_x$  est aussi dépilée) et  $R$  reste tel qu'il est. Sinon la valeur de  $R$  est affectée à  $P$ , cette même valeur devient la nouvelle tête de la deuxième pile et  $R$  est mise à 0.
  - Une station est désignée comme étant le moniteur, elle surveille le fonctionnement du réseau, exemples :
    - Le jeton libre fait plus d'un tour sans que la priorité ne redescende alors le moniteur purge l'anneau (trame PRG) et le jeton, est régénéré.
    - Une trame de données ayant fait plus d'un tour est éliminée par le moniteur.
    - Si aucune trame ne passe par le moniteur, au bout d'une certaine temporisation l'anneau est purgé et le jeton est re-généré.
- La surveillance de la présence du moniteur se fait grâce aux trames AMP ("Active Monitor Present") envoyés par le moniteur et surveillé par les autres



stations. L'élection du moniteur se fait de la façon suivante : une station ne recevant pas de trame AMP pendant un certain temps émet une trame CT ; une station recevant un CT le ré-émet si l'adresse de l'émetteur est plus grande que la sienne, sinon elle émet un CT ; au final, la station ayant la plus grande adresse MAC devient le moniteur.

L'insertion d'une station dans l'anneau se fait comme suit : la station émet des trames LMT ("Lobe Media Test") ; la station teste si elle est la première pour devenir le moniteur, si un moniteur est présent (AMP, PRG), la station émet une trame DAT ("Duplicate Address Test") ; si en retour les bits A et C sont non positionnés la station s'insère, sinon la station se retire. Si aucun moniteur n'est détecté, la station émet une trame CT, si en retour les bits A et C sont non positionnés la station devient le moniteur.

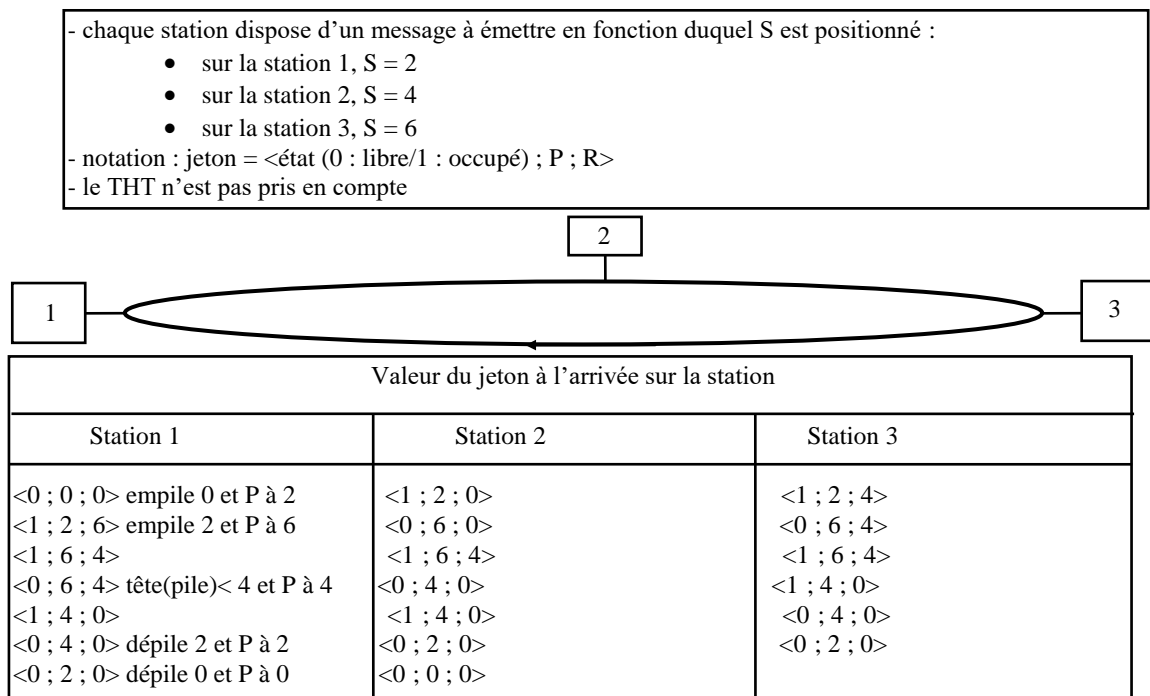


Figure 5 : exemple de fonctionnement de la méthode d'accès du jeton sur anneau

- Exemple : voir la figure 5.

#### II.4.2.2 Cas du jeton sur bus

Principales règles de fonctionnement ("token-bus »/IEEE802.4) :

- Chaque nœud maintient les adresses du prédécesseur et du successeur suivant un ordre décroissant (sauf entre deux nœuds) pour former un anneau logique.
- L'émetteur d'une trame a la possibilité de solliciter une réponse, auquel cas, le destinataire n'a pas besoin du jeton pour envoyer sa réponse.
- Lorsqu'un nœud passe le jeton, il reste à l'écoute pour vérifier que le nœud successeur envoie une trame (de données ou le jeton). Dans le cas négatif et après

un certain nombre de tentatives un nouveau successeur est élu. Dans une première phase, une requête est diffusée sur le réseau pour déterminer le successeur de l'ancien successeur ; si cette requête échoue un algorithme de résolution en arbre quaternaire est utilisé pour déterminer le nouveau successeur (l'adresse est de 48 bits, la profondeur de l'arbre est 24).

- De plus, pour prévenir la perte d'un jeton, chaque station maintient un temporisateur et au bout d'un délai de garde décrète que le jeton est perdu. Un algorithme pour désigner quel nœud doit re-générer le jeton (en fonction des adresses) est mis en place.

- ayant le jeton, un nœud teste périodiquement (tous les  $P$  passages du jeton,  $16 \leq P \leq 255$ ) s'il existe un nouveau nœud qui veut s'insérer dans l'anneau et devenir le successeur du nœud qui dispose du jeton. Si plusieurs nœuds veulent s'insérer un algorithme de résolution en arbre quaternaire est utilisé. L'insertion du nouveau nœud n'est effectuée que si le temps de rotation du jeton reste en dessous d'un temps de rotation cible. La station qui dispose du jeton invite à l'insertion en envoyant un sollicite-successor-1 (pour les adresses inférieures à la sienne, sinon sollicite-successor-2). Si pas de réponse la station passe le jeton. Si une seule réponse, alors insertion de la station. Si plusieurs réponses alors la station qui dispose du jeton envoie un resolve-contention. Une station qui veut s'insérer répond alors dans la  $K^{\text{ème}}$  fenêtre,  $K$  est déterminé en fonction de l'adresse. Toutefois si le canal est détecté occupé avant la  $K^{\text{ème}}$  fenêtre la station se retire (figure 6).

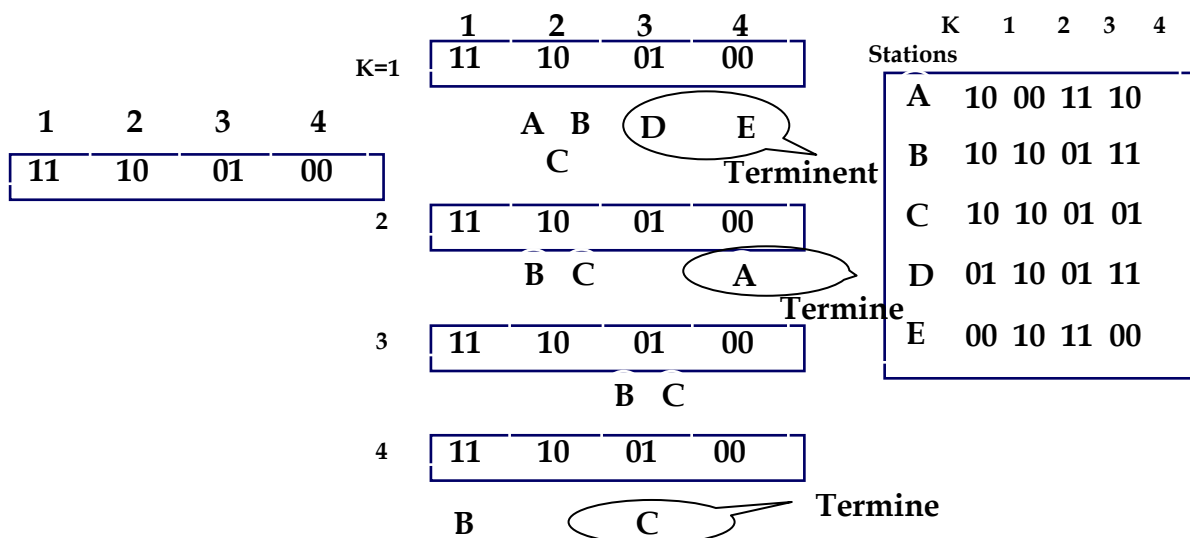


Figure 6 : Résolution de contention

- un mécanisme optionnel de priorité est mis en œuvre. S'il n'est pas utilisé, un nœud ne peut détenir le jeton au-delà d'une certaine période (fixée lors de la configuration). Autrement, à un message est associée une priorité. Quatre priorités sont définies. A chaque priorité  $I$  est associée un objectif de temps de

rotation du jeton  $OTR_I$ . Plus la priorité  $I$  est haute plus  $OTR_I$  est grand. Sur chaque nœud et pour chaque ordre de priorité  $I$  (à partir de la plus haute), lorsque le jeton revient, après un temps  $TR$ , les messages sont émis dans la limite du temps qui reste. La plus haute priorité 6 est utilisée pour le trafic temps réel qui garantit un temps d'accès inférieur  $N*OTR_6$ ,  $N$  est le nombre de stations.

- Exemple : voir la figure 7.

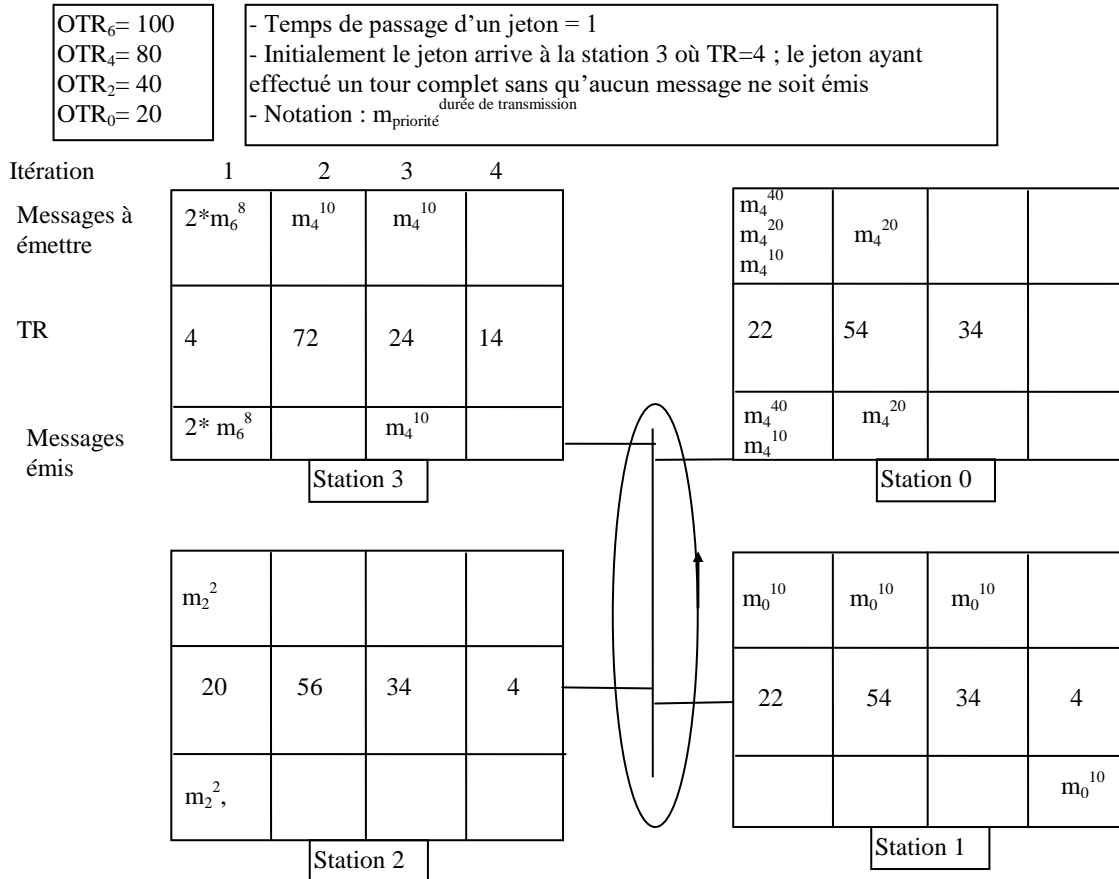


Figure 7 : exemple simplifié du fonctionnement de la méthode d'accès IEEE 802.4

### II.4.3 Technique de la tranche vide ou anneau en tranches ("empty slot" ou "slotted ring")

Cette technique a été élaborée pour un réseau en anneau. Le principe de cette technique consiste à faire tourner sur l'anneau un ensemble de trames ayant une taille fixe que l'on peut considérer comme des wagons ou encore des tranches de temps (vides ou pleines). Un nœud désirant émettre un message doit attendre le passage d'un wagon libre. Le message initial est découpé si nécessaire suivant la taille des wagons. Lorsqu'un coupleur voit passer un wagon transportant des données qui lui sont destinées, soit qu'il prélève ces données et libère le wagon, soit qu'il les copie et c'est

l'émetteur qui libère le wagon (acquiescement). En cas de défaillance, ceci peut se faire aussi par un nœud de contrôle. Si aucun mécanisme pour éviter la famine n'est mise en œuvre, le temps de réponse n'est pas borné.

La réalisation de cette technique est faite au niveau des coupleurs et en utilisant une technologie rapide pour pouvoir atteindre les débits escomptés (50 Mb/s). La taille des wagons est de quelques dizaines d'octets.

## **II.4.4 Les techniques à accès aléatoire**

### ***II.4.4.1 ALOHA***

La première technique, appelée ALOHA, à accès aléatoire a été développée pour un réseau à diffusion reliant les îles d'Hawaï. Le principe de l'accès aléatoire est le suivant. Tous les nœuds communiquent à travers une liaison multipoint. Le nombre de nœuds n'est pas limité. Lorsqu'un nœud a un message à émettre, il transmet le message. Les émissions de deux ou plusieurs messages risquent de se superposer. On dit alors qu'il y a eu collision entre ces messages. Le signal résultant sur le support est non interprétable et les messages en collision sont perdus. Ils doivent par la suite être retransmis.

L'accès aléatoire est ainsi décentralisé et n'impose pas une synchronisation préalable à une émission. Cependant les collisions ont pour conséquence une perte dans la bande passante d'autant plus importante que le nombre de nœuds augmente.

Une amélioration de l'ALOHA est l'ALOHA en tranches où le temps est subdivisé en des intervalles (tranches) correspondant à la transmission de morceaux de messages de tailles égales. Une émission n'est autorisée qu'en début de tranches. Ainsi lorsqu'une collision a lieu, elle est limitée à une tranche et si une partie d'un message a été correctement transmise, elle le sera durant le reste des tranches suivantes. On arrive ainsi à doubler le débit, mais cette technique est coûteuse à mettre en œuvre étant donné que les communications doivent être synchronisées.

Un nœud qui vient d'émettre un message, probablement va le faire suivre par une suite d'autres messages. Partant de cette constatation, une autre amélioration de l'ALOHA est la réservation de tranches de temps. L'idée a été alors de réunir les tranches en des trames d'une longueur supérieure au temps d'aller-retour. Ainsi chaque nœud peut savoir au début d'une tranche ce qui s'est passé dans la même tranche de la trame précédente. Si une tranche est libre ou en collision, la tranche correspondante est libre d'accès dans la trame suivante. Sinon, si un nœud réussit une transmission dans cette tranche, la tranche correspondante dans la trame suivante lui est réservée. Grâce à cette technique on peut arriver à un taux d'utilisation de la bande passante proche de 1.

#### **II.4.4.2 CSMA**

Dans le cas des LAN, on utilise aussi l'accès aléatoire mais d'autres techniques plus appropriées ont été élaborées. En effet le délai de propagation d'un signal est très faible et par conséquent un nœud écoutant le canal peut déterminer rapidement l'état du canal. Ces techniques sont dites à accès aléatoire avec écoute de la porteuse (CSMA : "Carrier Sense Multiple Access"). Avant d'émettre un message, un nœud doit se mettre à l'écoute du canal et ne transmettre que s'il ne détecte pas un signal sur la ligne. Ceci n'élimine pas la possibilité de collision étant donné le délai de propagation (figure 8). On définit la *période de vulnérabilité* comme étant le temps de propagation d'un signal entre les nœuds les plus éloignés. Durant cette période un coupleur peut ne pas détecter l'émission d'un signal par un autre nœud. De nombreuses variantes utilisant la méthode CSMA ont été proposées.

##### CSMA persistant :

Lorsque le canal est occupé, un coupleur désirant émettre un message poursuit l'écoute du canal jusqu'à ce qu'il soit libre et émet ensuite son message. Si une collision se produit, les stations attendent un temps aléatoire avant de retransmettre.

##### CSMA non persistant :

Lorsque le canal est occupé, un coupleur désirant émettre un message reprend l'écoute du canal après un temps aléatoire (cette procédure est réitérée jusqu'à ce que le canal soit libre).

##### CSMA P-persistant :

Le temps est divisé en slots, comme " Aloha discrétisé ". Si un coupleur veut émettre, il écoute pour savoir si le réseau est occupé. Si le réseau est libre (sinon il passe au slot suivant), il émet avec une probabilité  $p$ , et reporte l'émission au slot suivant avec une probabilité  $1 - p$ . Le processus continue jusqu'à ce que la trame soit émise. A la suite d'une collision il génère un temps aléatoire.

##### CSMA/CD (Collision Détection) :

A l'écoute du canal avant l'émission se rajoute l'écoute pendant l'émission pour déterminer s'il y a eu collision. Pour cela le signal émis est comparé au signal sur la ligne. Si une collision s'est produite, le coupleur abandonne l'émission et envoie une séquence de bits, appelée séquence de brouillage, pour faire persister la collision et assurer que les autres coupleurs se sont rendu compte de la collision. L'émission sera reprise après un temps aléatoire. L'émetteur devra rester à l'écoute du canal pendant une période (tranche canal) égale à deux fois le temps maximum de propagation d'un signal entre deux coupleurs. Au-delà de cette période, l'émetteur est sûr qu'il n'a pas subi de collision et qu'il n'en subira pas.

Contrairement aux méthodes précédentes l'émetteur s'assure du bon déroulement de l'émission sans attendre un acquittement mais par détection ou non, de collision.

L'avantage est de pouvoir abandonner l'émission dès qu'une collision est détectée et de ne pas attendre d'acquittement.

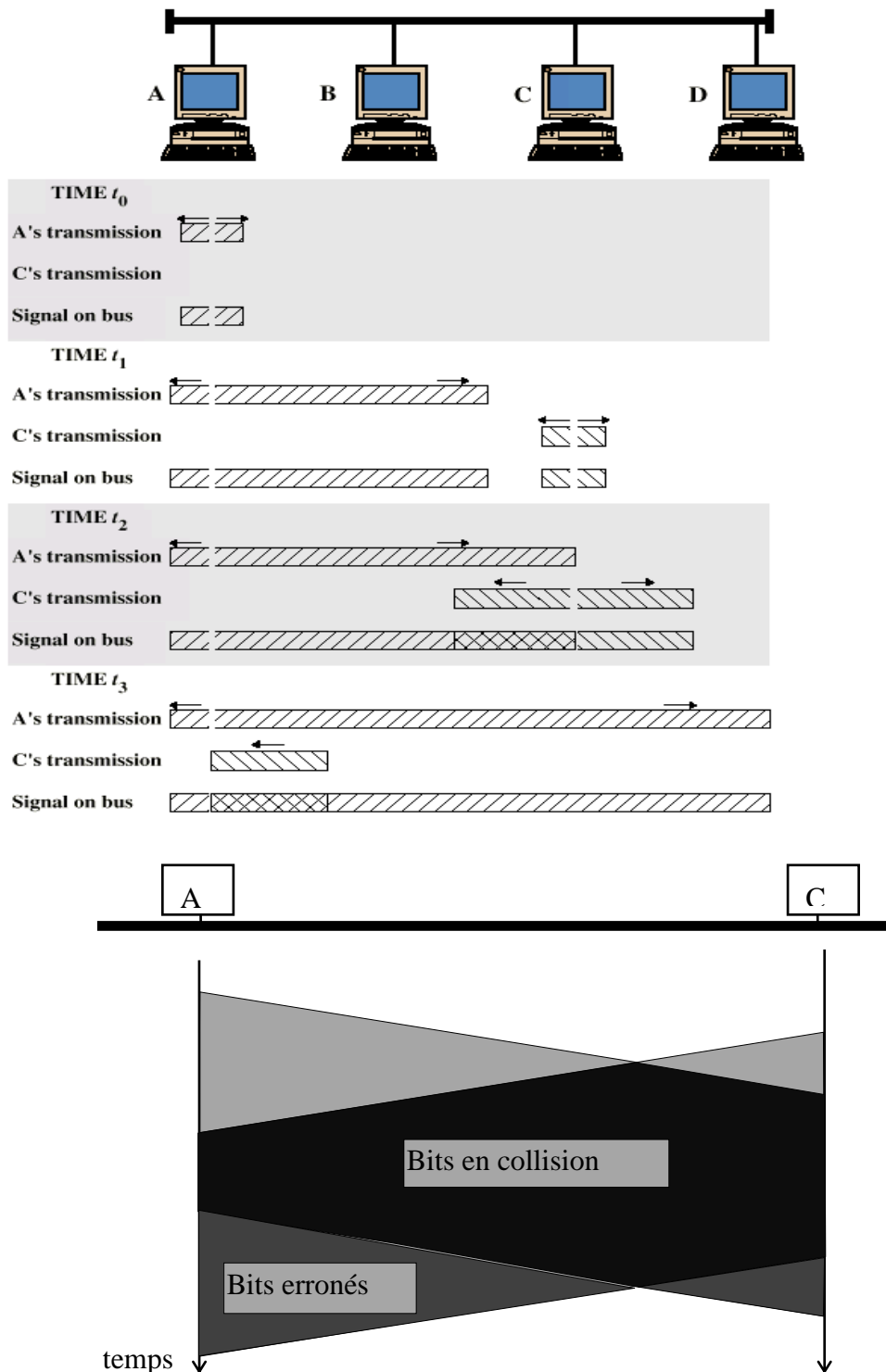


Figure 8 : collision entre deux émissions

Quelques applications numériques : méthode d'accès CSMA/CD, taille minimale d'une trame 512 bits

- pour un support métallique, débit du câble = 10 Mb/s, vitesse propagation = 200.000 Km/s

→ la tranche canal  $\leq 51,2 \mu\text{s}$ .

→ la longueur d'un segment  $\leq (51,2 \cdot 10^{-6} \cdot 2 \cdot 10^8) / 2 = 5,12 \text{ Km}$

- pour une fibre multimode, débit du câble = 10 Mb/s, la vitesse propagation = 100000 Km/s

→ la longueur d'un segment  $\leq 2,5 \text{ Km}$

- pour une fibre monomode, débit du câble = 10 Mb/s, la vitesse propagation = 250 000 Km/s

→ la longueur d'un segment  $\leq 6 \text{ Km}$

- on veut maintenant réaliser un réseau avec un débit = 100 Mb/s et en utilisant la fibre monomode

→ la tranche canal  $\leq 5,12 \mu\text{s}$ .

→ la longueur d'un segment  $\leq 600 \text{ m}$

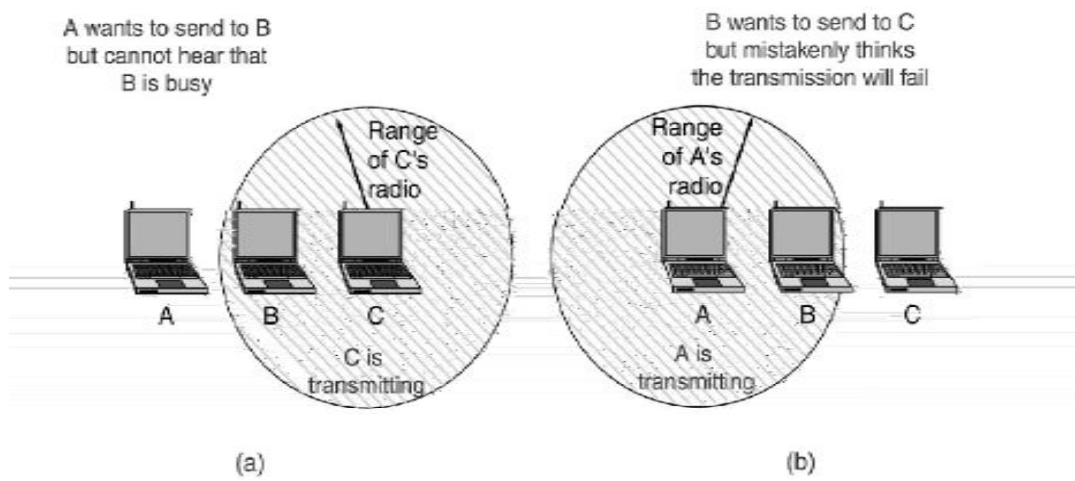
→ moins de nœuds

#### CSMA/CA (Collision Avoidance) :

Dans le cas des réseaux locaux sans fils WiFi, la méthode d'accès de base est appelée **DCF** « **Distributed Coordination Function** », c'est une méthode d'esquive de collision **CSMA/CA** « **CSMA/ Collision Avoidance** ». Dans un environnement sans fil, il n'est pas possible de s'assurer que toutes les stations s'entendent entre elles (ce qui est l'hypothèse de base du principe de détection de collision). Particulièrement se pose le problème de la station cachée (cf. figure 9-a), ce problème se produit quand deux stations A et C ne peuvent pas s'entendre l'une et l'autre (du fait par exemple d'une distance qui les sépare suffisamment importante) mais elles ont des zones de couverture qui se recoupent et où se trouve une station B. Si les stations A et C ne font que la détection de porteuse, n'étant pas en mesure de s'entendre l'une l'autre, elles vont s'autoriser à émettre des paquets en même temps à la station B ce qui provoque une collision entre les trames et donc leurs pertes. En outre, se pose aussi le problème de la station exposée (cf. figure 9-b) : la station B veut transmettre à C, B écoute le canal et le trouve occupé par A, B pense que le canal est occupé et il ne peut pas joindre C Alors que c'est possible.

Suivant le mode DCF, une station voulant transmettre écoute le support, et s'il est occupé, la transmission est différée. Si le canal est libre pour un temps spécifique (appelé **DIFS**, **Distributed Inter Frame Space**), alors la station est autorisée à transmettre. La station réceptrice va vérifier le **CRC** du paquet reçu et renvoie un accusé de réception (**ACK**). Si l'émetteur ne reçoit pas l'accusé

de réception, alors il retransmet le fragment jusqu'à ce qu'il l'obtienne l'ACK ou abandonne au bout d'un certain nombre de retransmissions.



(a) «station cachée »

(b) « station exposée »

Figure 9 : Problèmes de la station cachée et de la station exposée

Durant la transmission de la trame et jusqu'à réception de l'accusé de réception, NAV « Network Allocation Vector », aucune station n'a le droit d'émettre. Le temporisateur NAV est le premier élément qui permet concrètement d'éviter les collisions et correspond à un indicateur de "Virtual Carrier Sense".

Ce principe est appliqué dans le cas des trames courtes, pour les trames longues une réservation du canal se fait d'abord moyennant des messages courts (RTS/CTS: "Request To Send/Clear To Send").

Si le canal est libre pendant DIFS, une station émettrice transmet un RTS et attend que le destinataire réponde par un CTS. Toute station qui entend le CTS doit déclencher le NAV. Aussi, toute station recevant le RTS, déclenchera le NAV (figure 10). Ce mécanisme réduit la probabilité de collision par une station « cachée » de l'émetteur dans la zone du récepteur à la courte durée de transmission du RTS. Un algorithme de back-off (BO), est utilisé pour éviter que deux stations émettent en même temps (comparable à celui du CSMA/CD). Le seul cas où le back-off n'est pas utilisé est quand la station décide de transmettre une nouvelle trame et que le support a été libre pour DIFS.

**Remarque :** Il existe un autre IFS appelée PIFS « Point coordination IFS » dont la durée est de  $78\mu s$  (SIFS+Slot), il est utilisé par la méthode de polling PCF au lieu du DIFS, il permet de donner une priorité au AP. L'ordre de priorité conséquent est induit par : SIFS<PIFS<DIFS.



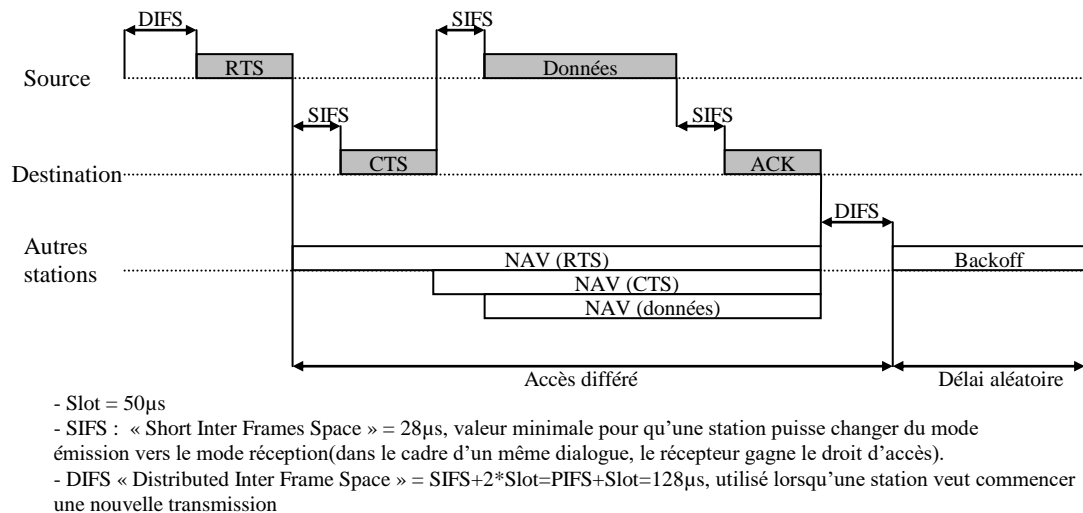


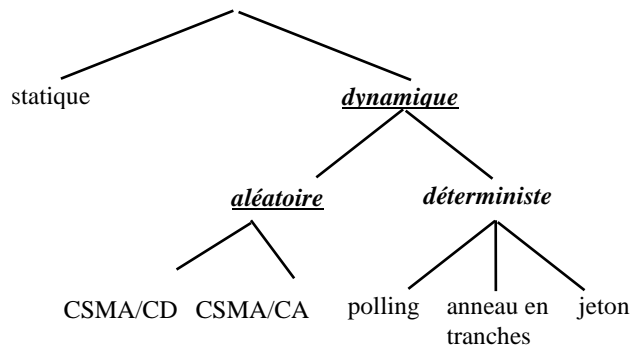
Figure 10 : transmission CSMA/CA & "Virtual Carrier Sensing"

### Protocoles sans collision

- Cas du protocole bit-map : dans ce protocole, chaque station utilise un mini-slot pour annoncer qu'elle souhaite transmettre une trame (bit à 1) ou non (bit à 0). Toutes les stations entendent cette annonce. Une fois que toutes les stations ont effectué leur annonce (leur nombre doit être connu de tous), les transmissions ont lieu dans l'ordre des stations ayant annoncé une trame. Il n'y a pas de collision.
- Cas du protocole à comptage binaire : pour limiter la période de contention dans le protocole précédent, on peut utiliser un identificateur unique des stations. S'il y a N stations,  $\log_2 N$  bits peuvent suffire. Chaque station qui veut transmettre une trame annonce les bits de son identification, un par mini-slot dans la phase de contention. On suppose que le canal réalise un « ou » logique. Si une station « entend » un bit différent de celui qu'elle a émis, elle se retire de la compétition. À la fin, seule une station reste, et a le droit de transmettre dans la période de transmission qui suit. Un protocole similaire, nommé CSMA-CR (Contention Resolution) est mis en œuvre dans le RNIS (interface S).

### II.4.5 Classification

Toutes les techniques citées ci-dessus sont dynamiques (adaptatives) et le partage du support est temporel, seule la technique du « polling » est centralisée. Une classification de ces techniques d'accès est décrite par la figure 11.



*Figure 11 : classification des techniques d'accès utilisées dans les LAN*

## **II.4.6 Comparaison**

Plusieurs études d'évaluation de méthodes d'accès ont été effectuées. Nous retenons dans la suite les principaux résultats obtenus.

La méthode CSMA/CD dépend essentiellement du nombre de nœuds émetteurs, de la charge de communication provenant des différents coupleurs et du rapport temps de propagation sur le support divisé par le temps de transmission (dépôt) d'une trame. Lorsque ces deux paramètres augmentent le nombre de collisions augmentent et par conséquent l'utilisation effective diminue. On estime dans le cas d'un réseau Ethernet (10Mb/s) que le débit imposé au réseau (y compris les retransmissions) ne doit pas dépasser 5Mb/s s'il y a plus de 100 nœuds en émission, au risque que le débit réel s'écroule. Ceci n'est pas le cas pour les techniques à jeton qui sont moins sensibles à la charge imposée.

Dans le cas de la méthode CSMA/CD, lorsque la charge d'émission est faible, et donc le taux de collision, les temps d'attente pour obtenir l'accès au support sont faibles. Dans le cas des techniques à jeton, ce temps dépend de la taille de l'anneau et du temps de traversé d'un coupleur. Si un seul nœud émet des messages l'efficacité est inférieure à celle de la méthode CSMA/CD.

Un autre paramètre dont dépend la méthode CSMA/CD et la taille maximale des trames, plus elle est petite, plus le découpage des messages conduit à un nombre important de trames et donc de collisions. Inversement si cette taille augmente, les temps d'attente de libération du support de transmission augmentent, l'accès étant aléatoire, d'où le risque qu'un nœud reste en attente de la libération du support d'une façon inacceptable. Dans le cas des techniques à jeton ce problème ne se pose pas pourvu que le jeton ne soit pas détenu par un nœud que pendant une certaine durée limite (ce qui revient à limiter la taille d'une trame).

L'évaluation des performances de ces méthodes sera traitée dans les exercices qui suivent.

## II.5 Exercices

### Exercice 1

On considère la méthode d'accès ALOHA. Les trames sont générées suivant le processus de Poisson.

On définit les paramètres suivants :

- T: durée de trame (taille moyenne d'une trame / débit) ;
- g : le nombre moyen de trames produites par seconde par l'ensemble des nœuds.
- s : le nombre moyen de trames émises sans collision par seconde ;

On pose :

- S = s.T (débit utile normalisé)
- G = g.T (charge globale normalisée)

La probabilité d'émettre k trames pendant une durée T (notée  $P_k(T)$ ) est donc :

$$P_k(T) = \frac{(gT)^k}{k!} e^{-gT}$$

- 1) Quelle est la condition pour qu'une trame soit émise avec succès à un instant t ? Déduire la probabilité de succès  $P_{\text{succès}}$ .
- 2) Déterminer la probabilité de succès  $P_{\text{succès}}$  en fonction de s et g.
- 3) Déterminer S en fonction de G.
- 4) Dans le cas de l'Aloha Slotté, que devient l'expression de S en fonction de G.
- 5) Tracer S en fonction de G.

### Exercice 2

On considère un réseau local utilisant la méthode d'accès aléatoire CSMA où chaque station dispose toujours d'un message à transmettre. Lorsqu'une station détecte que le support est libre, elle transmet une trame avec une probabilité P. La probabilité qu'une seule station, à la fois, émette une trame est donc :

$$P_u = N \cdot P \cdot (1-P)^{N-1}.$$

On définit les paramètres suivants :

- C = débit de transmission du support,
- D = délai de propagation d'un signal sur le support de transmission,
- L = longueur d'une trame (supposée toujours constante),
- N = nombre de stations dans le réseau,
- U = utilisation du réseau.

On pose :  $F = D \cdot C / L$

Une unité de temps est égale à la tranche canal ( $2 \cdot D = 1$ ). Une collision est traitée en une tranche canal.

- 1) Montrer que la valeur  $1/N$  de la probabilité  $P$  réduit la probabilité de collision lors d'une émission ? Cette valeur sera choisie dans ce qui suit.
- 2) Que représente  $F$  ?
- 3) Déterminer le temps d'injection en fonction de  $F$ .
- 4) Déterminer le temps moyen perdu séparant deux émissions réussies (on suppose que le temps perdu sans qu'aucune station n'émette fait partie de ce temps perdu).
- 5) En ne considérant que les temps nécessaires pour l'injection d'une trame et la propagation d'un signal, déterminer l'utilisation  $U$  en fonction de  $F$  et  $N$ .
- 6) Dédire la valeur de  $U$  quand  $N$  tend vers l'infini (sachant que lorsque  $N$  tend vers l'infini  $(1-(1/N))^{N-1}$  tend vers  $(1/e)$ ). Que peut-on conclure ?
- 7) Pour  $F=0.1$  et  $F=2$  tracer l'allure de la courbe  $U$  en fonction de  $N$ .
- 8) Pour  $N=2$  et  $N=10$  tracer l'allure de la courbe  $U$  en fonction de  $F$ .

### Exercice 3

On considère un réseau local Token-Ring où chaque station dispose toujours d'un message à transmettre. L'émetteur d'une trame libère le jeton dès que le premier bit de la trame lui revient et une fois qu'il a fini de transmettre la trame courante. Le temps d'injection du jeton est supposé nul. On définit les paramètres suivants :

- $C$  = débit de transmission du support (débit de transmission),
- $D$  = délai de propagation d'un signal sur le support de transmission,
- $L$  = longueur d'une trame (supposée toujours constante),
- $N$  = nombre de stations sur le réseau,
- $U$  = utilisation du réseau.

On pose :  $F = D \cdot C / L$

On note que le temps de propagation du jeton d'une station vers la suivante est égal à  $D/N$ .

- 1) Que représente  $F$  ?
- 2) Une unité de temps est choisie égale à  $L/C$  ( $L/C=1$ ). En ne considérant que les temps nécessaires pour l'injection d'une trame et la propagation d'un signal, déterminer l'utilisation  $U$  en fonction de  $F$  et  $N$ , dans chacun des deux cas suivants :  $F \leq 1$  et  $F \geq 1$

On remarque que l'utilisation  $U$  correspond ici au rapport entre le temps utile pour l'injection d'une trame et le temps total pour émettre une trame et passer le jeton à la station suivante.

- 3) Comment varie  $U$  par rapport à  $N$  ? Déduire la valeur de  $U$  quand  $N$  tend vers l'infini. Que peut-on conclure ?
- 4) Pour  $F=0.1$  et  $F=2$  tracer l'allure de la courbe  $U$  en fonction de  $N$ .
- 5) Pour  $N=2$  et  $N=10$  tracer l'allure de la courbe  $U$  en fonction de  $F$ .
- 6) Comparer ces courbes avec ceux de l'exercice précédent.

### III. Normalisation des réseaux locaux

La diversité des LANs, de part les techniques et les moyens mis en œuvre, a conduit à un besoin de normalisation, d'autant plus que les LANs peuvent comporter une grande variété d'équipements provenant de différents constructeurs. C'est ainsi que le comité 802 de l'IEEE (« Institute of Electrical and Electronic Engineers ») a été constitué en 1980. La normalisation concerne les couches 1 et 2 du modèle de référence OSI. Une famille de normes a été élaborée. Tous les travaux ayant aboutis du comité IEEE 802 ont été repris sous forme de norme ISO sous les numéros 8802.x. Des travaux similaires à ceux du comité IEEE 802 ont été menés en Europe par l'ECMA (« European Computer Manufacturers Association »).

#### III.1 Les normes IEEE 802

Les normes IEEE 802.x correspondent à une implémentation spécifique aux LANs et plus généralement aux couches physique et liaison. L'architecture IEEE 802 est décrite par la figure 1.

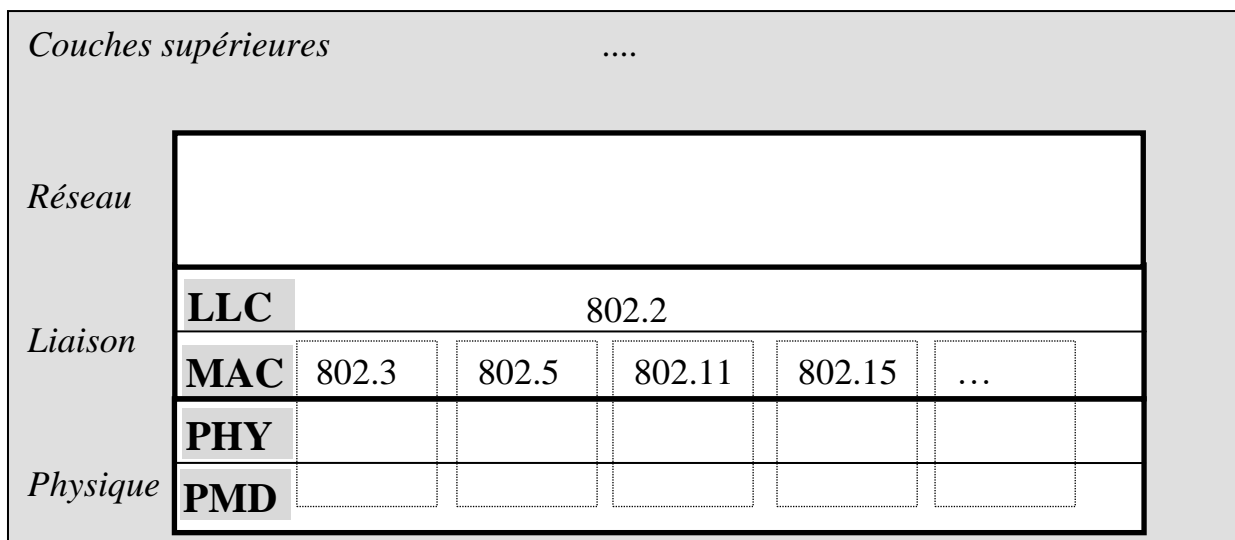


Figure 1 : architecture IEEE 802

La norme IEEE 802.1 montre comment l'architecture IEEE 802 s'articule avec le modèle de référence OSI. Parmi les thèmes traités par la norme IEEE 802.1 nous retrouvons : l'architecture des LAN/MAN, l'interconnexion avec les réseaux 802, la gestion des réseaux 802 ... La couche liaison est décomposée en deux sous-couches : une couche pour le contrôle d'accès (MAC : "Medium Access Control") et une couche pour le contrôle de liaison (LLC : "Logical Link Control"). Cette norme définit les différentes primitives fonctionnelles en particulier ceux relatives aux interfaces avec les couches supérieures et à la gestion du réseau (interconnexion et algorithmes de filtrage, adressage, administration).

La couche physique quant à elle est composée de deux sous-couches : la couche PHY et la couche PMD (« Physical MeDium »). La couche PMD définit le type de support, le type de connecteur, le mode de transmission ... Cette couche réalise aussi, dans le cas du protocole CSMA/CD, l'écoute du signal. La couche PHY, quant à elle, réalise la conversion parallèle / série et inversement, un contrôle d'erreur (différent de celui effectué au niveau MAC), le codage en ligne pour faciliter la synchronisation ...

Les normes IEEE 802.3 802.4 802.5 décrivent différentes méthodes d'accès et les caractéristiques physiques rattachées à chacune de ces méthodes :

- IEEE 802.3 se base sur la méthode CSMA/CD sur bus, elle concerne les réseaux Ethernet.
- IEEE 802.4 se base sur la méthode jeton sur bus (dissous),
- IEEE 802.5 se base sur la méthode jeton sur anneau, elle a été introduite par IBM (réseaux Token-Ring).
- La norme IEEE 802.6 (dissous) est relative aux réseaux métropolitains (MAN). Elle est remplacée particulièrement par le Gigabit Ethernet utilisé dans de nombreux MAN.
- La norme IEEE 802.11 concerne les réseaux locaux sans-fil WLAN ("Wireless LAN"), elle se décompose en plusieurs normes de transmission, offrant chacune des caractéristiques différentes en terme de fréquence, de débit ou de portée du signal radio.
- La norme IEEE 802.15 (Bluetooth) est une technologie de réseaux personnels sans fils (WPAN), elle est destinée à simplifier les connexions entre : ordinateurs imprimantes, téléphones portables, appareils domestiques, oreillettes sans fils, souris, clavier ... Cette technologie utilise un circuit radio de faible coût avec une faible consommation électrique.

Dans ce chapitre sont décrites les normes associées aux réseaux Ethernet et WiFi. Les deux sous-sections suivantes décrivent l'adressage au niveau MAC et la norme IEEE 802.2.

### III.1.1 Adressage MAC

Les liaisons n'étant pas point à point, une trame doit donc comporter l'adresse destination. Nous décrivons dans ce qui suit les différents modes d'adressages utilisés dans les trames MAC. Une adresse est attribuée à chaque coupleur.

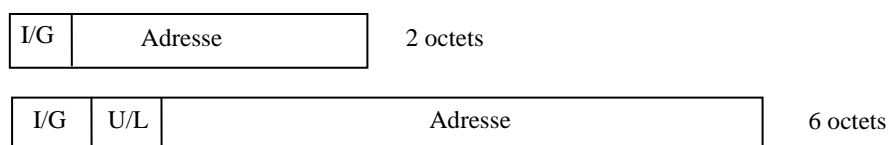


Figure 2 : formats d'adresses (LSB : « Less Significant Bit<sup>1</sup> »)

On distingue deux formats (figure 2). Le format court de longueur 2 octets (actuellement il n'est plus utilisé) et le format long de longueur 6 octets. Pour ces deux formats d'adresse le premier bit à gauche, de poids le plus faible, (bit I/G) indique s'il s'agit d'une adresse de

---

<sup>1</sup> C'est le bit le moins significatif (poids faible) qui est transmis le premier

groupe (G=1) ou individuelle (I=0). Tous les bits sont à 1 pour une diffusion. Dans le cas du format long, le second bit à gauche (bit U/L) indique si l'adresse est locale (L=1) ou universelle (U=0). Une adresse est locale si elle est attribuée par l'administrateur du réseau. Elle est dite universelle si elle est gérée par une entité internationale (dépendant de l'IEEE). Elle est alors divisée en deux parties. Les 3 octets de gauche servent à désigner le constructeur (OUI : « Organizationally Unique Identifier »), les 3 autres octets sont attribués par le constructeur et représente un numéro de série.

Exemples :	CISCO	00:00:0C:XX:XX:XX
	LANBridge de DEC	09:00:2B:XX:XX:XX

### **III.1.2 La norme IEEE 802.2**

Elle est relative au contrôle de liaison logique (LLC : "Logical Link Control"). La sous-couche LLC offre la possibilité de définir des liaisons de données logiques entre toute paire de nœuds, elle permet de masquer la méthode d'accès. Trois types de service ont été prévus :

- LLC 1 : sans connexion, non fiable,
- LLC 2 : avec connexion, conservation de l'ordre d'émission, fiable,
- LLC 3 : sans connexion, la récupération des erreurs est décidée par l'émetteur.

Etant donné le faible taux d'erreurs dans les LAN, le service LLC1 est le plus utilisé. Les erreurs résiduelles sont donc laissées à la charge des couches supérieures (exemple : TCP/IP). En outre le service LLC1 permet la diffusion. Lorsqu'il s'agit d'effectuer des échanges pendant une longue durée tout en garantissant le traitement des erreurs et en délivrant les messages en séquence (exemple d'application : transfert de fichiers), il convient d'utiliser le service en mode connecté LLC2. Le protocole LLC 2 est assez semblable à HDLC. Le service LLC3, plus simple à réaliser, est utile lorsque les échanges de données sont occasionnels mais doivent être fiables comme c'est le cas pour les réseaux locaux industriels. En particulier, ce service est utilisé pour réaliser un mécanisme de « polling ». Les services LLC2 et LLC3 ne s'utilisent qu'en point à point.

Une trame LLC, appelée LPDU : "Link Protocol Data Unit", comporte les champs suivants (figure 3) :

- 1 octet : adresse du point d'accès destination (DSAP : "Destination Service Access Point") ; le bit de poids le plus faible (I/G) indique si l'adresse est individuelle ou de groupe (LLC1) ; le bit suivant indique si l'adresse est attribuée par un organisme de normalisation (exemples, X25 : 0x7E, IP : 0x06, etc) ou non ;
- 1 octet : adresse du point d'accès source (SSAP : "Source Service Access Point") ;
- 1 ou 2 octets : contrôle (similaire à HDLC) ;
- jusqu'à 8 Octets de données.



DSAP	SSAP	Contrôle	Données
------	------	----------	---------

Le champ contrôle :

I-Frame (information)	0	N (S)							P/F	N (R)									
S-Frame (supervisory)	1	0	S	S	X	X	X	X	P/F	N (R)									
(Receive ready) RR	1	0	0	0	0	0	0	0	P/F	N (R)									
(Reject) REJ	1	0	0	1	0	0	0	0	P/F	N (R)									
(Receive not ready) RNR	1	0	1	0	0	0	0	0	P/F	N (R)									
U-Frame (unnumbered)	1	1	M	M	P/F	M	M	M											
	1	1	1	1	P	1	1	0	SABME command (set ABM mode extended)										
	1	1	0	0	P	0	1	0	DISC command (disconnect)										
	1	1	1	0	F	0	0	0	UA response (unnumbered acknowledge)										
	1	1	1	0	F	0	0	0	DM response (disconnect mode)										
	1	1	1	0	F	0	0	0	FRMR response (frame reject)										
	1	1	0	0	P	0	0	0	UI command (unnumbered information)										
	1	1	0	0	P/F	1	1	1	TEST cmd/rsp (test)										
	1	1	1	0	P/F	0	0	0	XID cmd/rsp (exchange identification)										
	1	1	1	0	P/F	0	0	0	AC0 cmd/rsp (information/acknowledge sequence 0)										
	1	1	1	0	P/F	0	0	0	AC1 cmd/rsp (information/acknowledge sequence 1)										

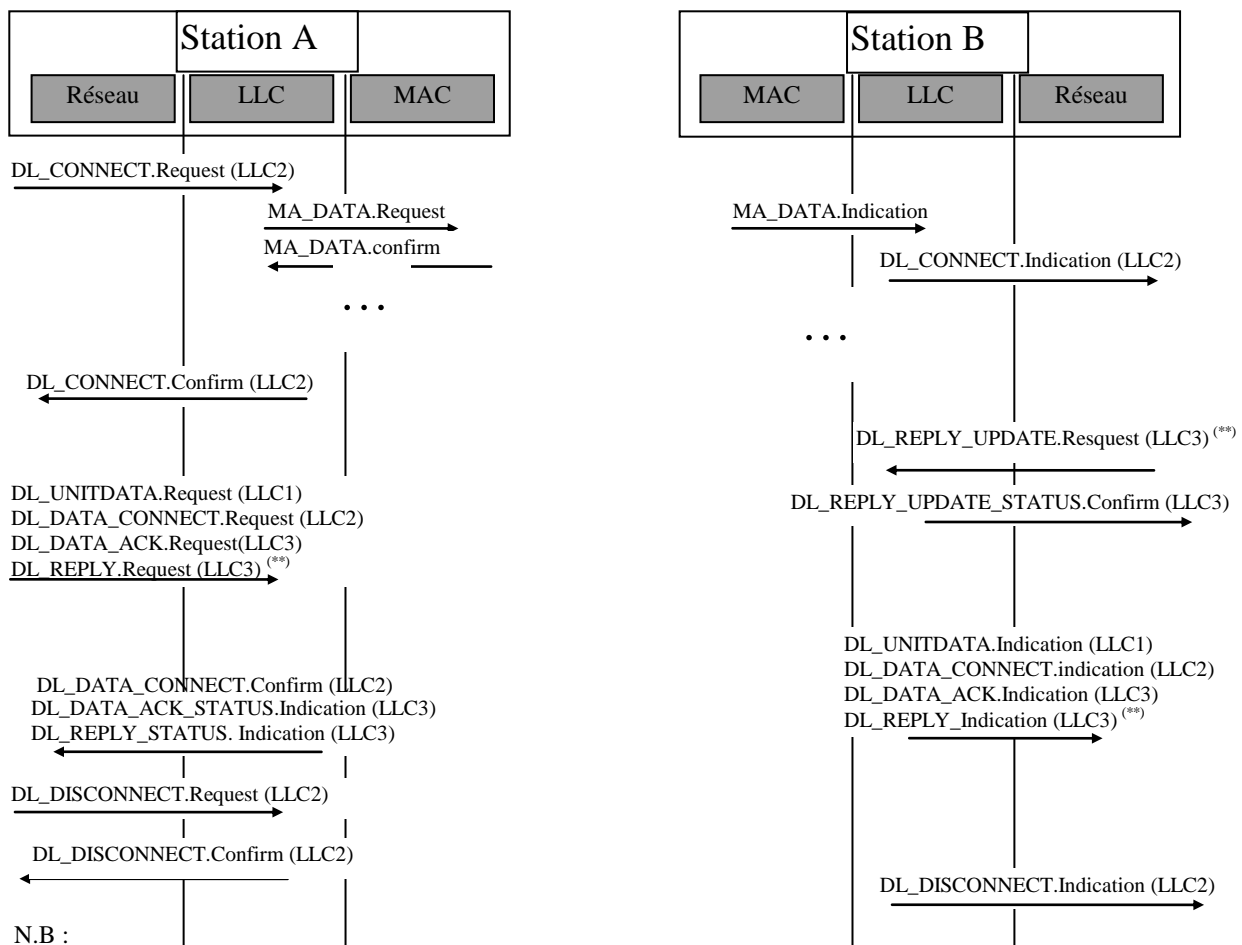
Figure 3 : format d'une trame LLC

Cette trame est encapsulée dans le champ des données de la trame MAC.

LLC1 utilise les LPDUs non numérotés suivants : UI («Unnumbered Information»), XID («eXchange Identification») et TEST. LLC 2 utilise le mode ABM (Asynchronous Balanced Mode). Le protocole de gestion des transmissions est donc de type Go-Back-N. Le protocole Selective-Repeat n'a pas été retenu étant donnée sa complexité et que les temps de transmissions dans les LAN sont assez faibles. LLC3 utilise des LPDU, inexistantes dans HDLC, AC0 et AC1 («Acknowledged Connectionless»). Le contrôle de flux et de type «stop-and-wait». Les primitives de services de LLC1 sont (Figure 4) :

- DL\_UNITDATA.request (@locale, @distante, LSDU, priorité)
- DL\_UNITDATA.indication (@locale, @distante, LSDU, priorité)

où : @locale et @distante permettent de déduire le SSAP et le DSAP et les adresses MAC ; LSDU (Link Services Data Unit) représente les données à envoyer ; priorité est utilisée dans le cas où la couche MAC gère des priorités.



N.B :

- Les primitives MAC ne sont pas toutes représentées dans la figure
- Les primitives DL\_REPLY\_X permettent au récepteur de renvoyer des données en réponse, en même temps que l'ack.
- Les primitives LLC2 pour le contrôle de flux ne sont pas représentées
- Les primitives STATUS sont équivalentes à une confirmation

Figure 4 : exemples d'échange de primitives LLC

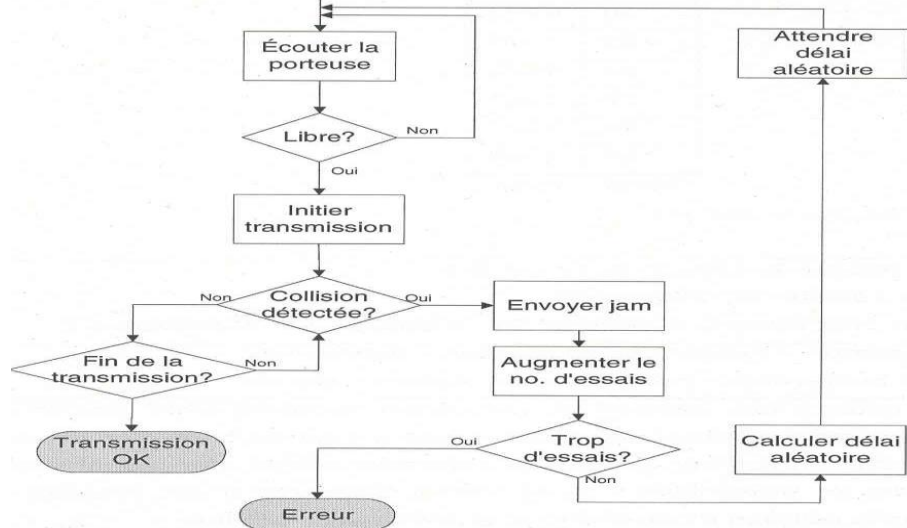
D'autres primitives de services pour LLC2 et LLC3 sont utilisées notamment pour l'établissement / libération de connexion et l'acquittement. La figure 4 donne un exemple d'échange de primitives entre les couches MAC, LLC et réseau. Les primitives de la couche physique ne sont pas représentées (PHY\_DATA.request, PHY\_DATA.indication).

### III.2 Les normes IEEE 802.3

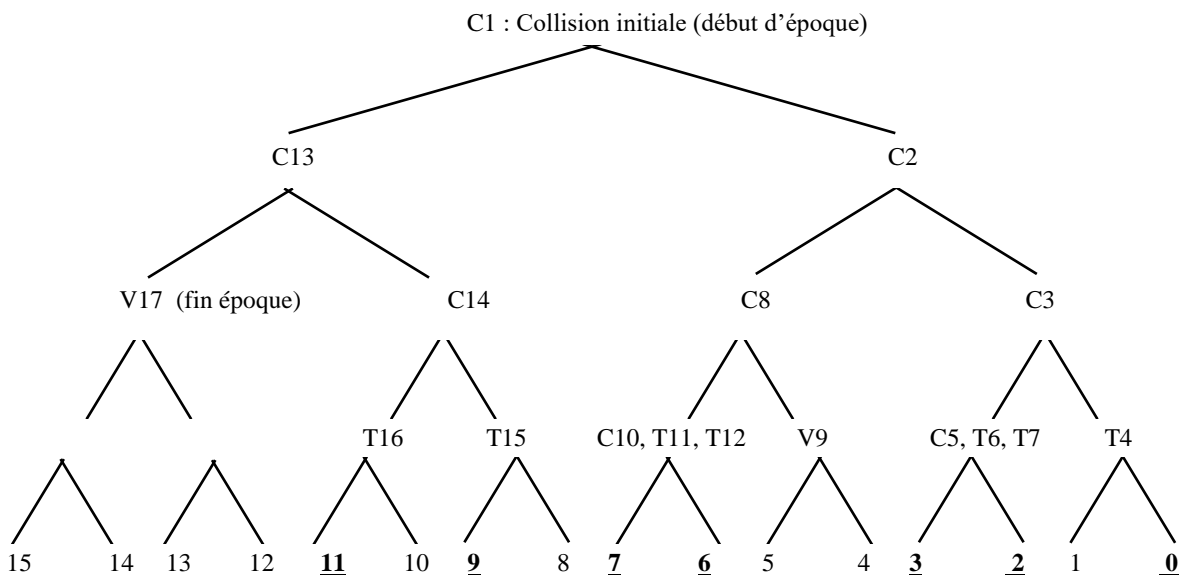
### III.2.1 Méthode d'accès

- CSMA/CD (cf. §II.4.4).
- à la suite d'une collision l'algorithme de reprise, appelé BEB ("Binary Exponential Backoff"), est le suivant : à la N<sup>ième</sup> collision et tant que N est inférieur à 16, on tire une valeur entière aléatoire V appartenant à  $[0..2^{\min(N,10)}[$  ; la nouvelle tentative sera effectuée après  $V * 51,2 \mu s$  ( $V * \text{Time\_Slot}$ ). Si le nombre de tentatives atteint 16, la transmission de la trame est abandonnée.
- un autre algorithme de reprise déterministe est utilisé pour le protocole 802.3D (DCR : « Deterministic Collision Resolution »). Il assure un délai maximum de

transmission. L'algorithme est basé sur le principe de résolution en arbre binaire (figure 5). On distingue deux modes, *le mode fermé* où les nouveaux messages arrivant à la suite d'une collision sont transmis après la résolution de la collision, et *le mode ouvert* où de nouveaux messages peuvent être transmis au cours de la résolution de la collision (si l'ordre d'un message n'est pas dépassé au niveau de l'arbre de résolution).



Ti : transmission d'un message  
 Ci : collision  
 Vi : aucune transmission (tranche vide)  
 où i est le numéro de tranche  
N : noeud N ayant un message à transmettre



Borne d'une époque =  $N * T + (N-1) * TC$  avec :  
 N : nombre de noeuds ; T : temps de transmission d'une trame ; TC : tranche canal

Figure 5 : résolution par un arbre binaire

### III.2.2 Format d'une trame

7 octets à 01010101	préambule utile pour la synchronisation
1 octet à 10101011	SFD ("Start Frame Delimiter")
2 ou 6 octets	adresse destination
2 ou 6 octets	adresse source
2 octets	longueur du champ information
46 à 1500 octets	champ information et bits de bourrage
4 octets	FCS sur les champs après le SFD

### III.2.3 Primitives de service

- MA\_UNITDATA.Request (*adresse\_destination, adresse\_source, MA\_SDU*) ;
- MA\_UNITDATA-STATUS.indication<sup>1</sup>(état (transmission\_OK, collisions\_excessives))
- MA\_UNITDATA.Indication (*adresse\_destination, adresse\_source, MA\_SDU, état* (Reception\_OK, longueur\_incorrecte, erreur\_FCS, erreur\_alignement))

### III.2.4 Principales caractéristiques physiques

Suivant le mode de transmission et la nature du support de transmission plusieurs normes de niveau physiques sont définies, elles sont décrites dans les sections IV.1.2 et IV.1.3.

### III.2.5 Evolutions de l'Ethernet vers le haut débit

D'autres normes ont été par la suite proposées pour augmenter le débit des LAN Ethernet :

- Le Fast Ethernet (100 Mb/s) est un aménagement de la norme IEEE 802.3, il garde le même protocole d'accès mais réduit le diamètre du réseau d'un facteur d'environ 10, il préconise 3 standards : le 100 BASE 4T sur de l'UTP 3/4/5 sur 4 paires, le 100 BASE TX sur de l'UTP 5 sur 2 paires et le 100 BASE FX sur 2 fibres multimodes.
- Utilisation d'un nouveau protocole MAC de type polling, les mêmes câbles téléphoniques sont gardés (« Voice Grade ») 4 paires sont cependant utilisées. Les travaux correspondants sont effectués par le comité IEEE 802.12 (100 BASE VG).
- Le Gigabit Ethernet (IEEE 802.3z, 802.3ab) a été défini dès le départ en deux versions, semi-duplex et duplex intégral. Dans la version semi-duplex (HD : Half-Duplex) le support est partagé et l'accès au support est géré par le même protocole CSMA/CD. Pour assurer la compatibilité avec les couches supérieures, la taille minimale des trames est maintenue à 64 octets par rapport à ces couches. Toutefois, afin de garder une longueur raisonnablement élevée pour le support partagé, les trames de taille inférieure à 512 octets sont complétées par des octets vides (*padding* ou *carrier extension*) pour atteindre les 512 octets (à la suite du FCS). Après l'envoi de cette première trame qui permet à un équipement d'occuper le support partagé, ce même équipement a la

---

<sup>1</sup> MA\_UNITDATA.confirm

possibilité d'envoyer d'autres trames, de taille inférieure cette fois-ci à 512 octets, pour une durée qui correspond à 8192 octets. Cette procédure de « réservation » temporaire du support par une trame de taille supérieure ou égale à 512 octets permet d'assurer un débit utile élevé même si les trames de faible taille (<512 octets) dominent. La taille maximale des trames est la même que pour Ethernet. La version duplex-intégral (FD : Full-Duplex) de Gigabit Ethernet permet d'interconnecter des équipements à travers un support bidirectionnel (débit théorique 2x1 Gbit/s), utilisé par deux équipements à la fois, donc CSMA/CD devient inutile. En pratique, la version FD est celle commercialisée. Elle permet de s'affranchir des contraintes de « *time slot* » et donc d'augmenter la taille maximale du réseau jusqu'aux limites imposées par la technologie de transmission (3000 m pour 1000 Base-LX sur fibre monomode).

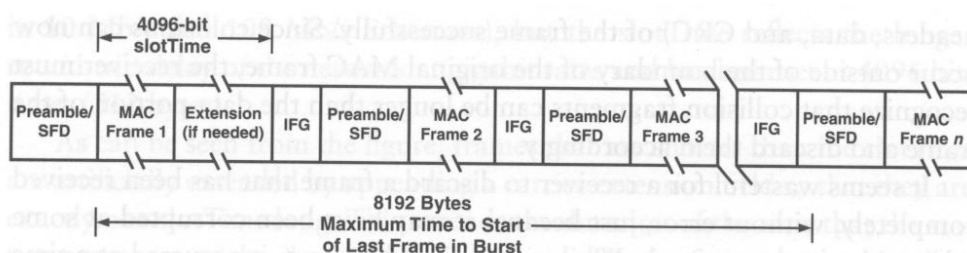


Figure 10-6 Frame bursting.

- Utilisation des commutateurs rapides.
- L'Ethernet a évolué vers des débits de plus en plus élevés, vers le recours à la commutation uniquement et est devenu utilisé non plus et uniquement à l'échelle LAN mais aussi MAN/WAN, le tableau suivant résume cette évolution.

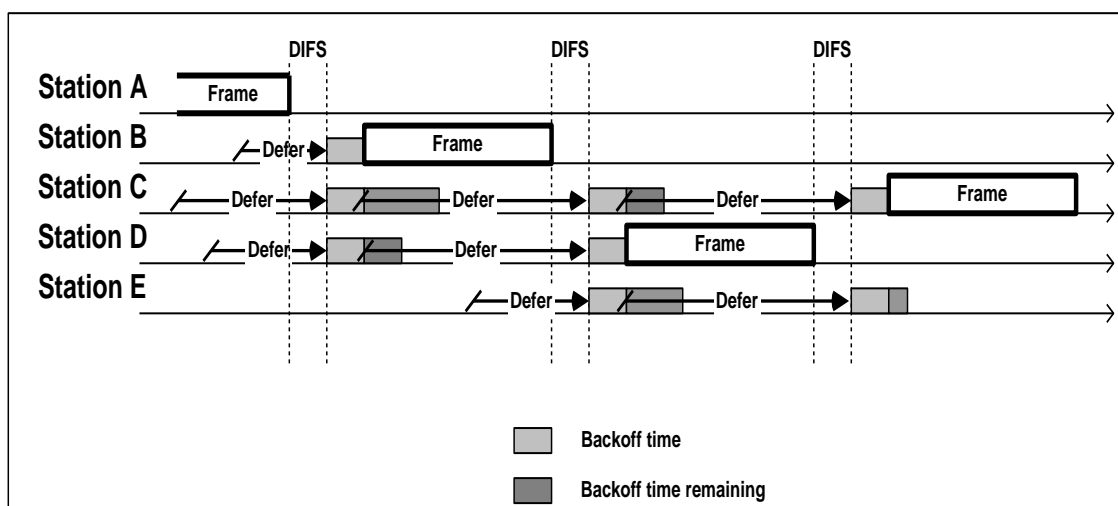
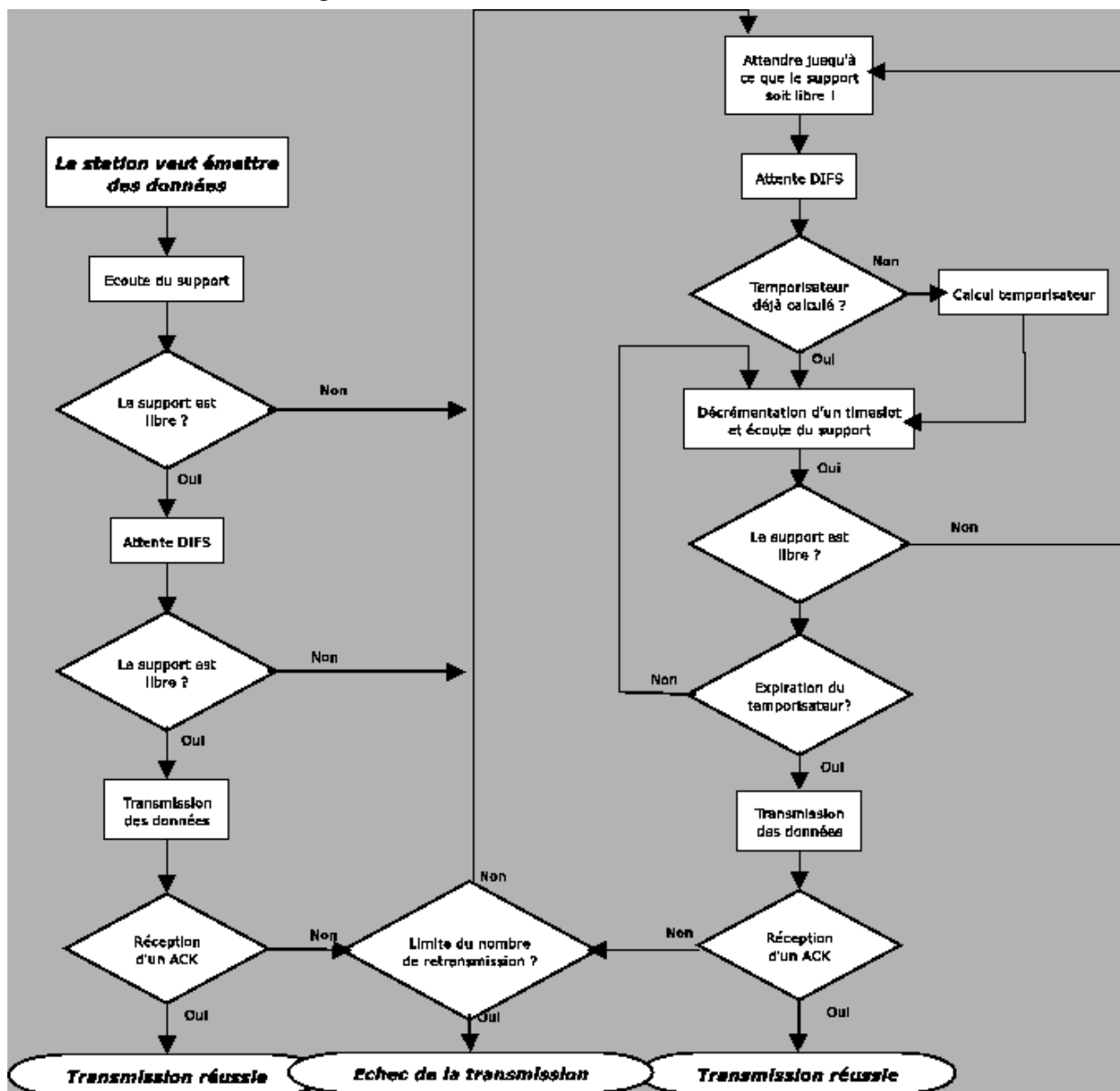
<b>Supplément</b>	<b>Année</b>	<b>Description</b>
802.3a	1985	10 BASE-2 thin Ethernet
802.3c	1985	10 Mbps repeater specification
802.3d	1987	Fiber Optic Inter Repeater Link
802.3i	1990	10 BASE-T twisted pair
802.3j	1993	10 BASE-F fiber optic
802.3u	1995	100 BASE-T Fast Ethernet and auto negotiation
802.3x	1997	Full duplex standard
802.3z	1998	1000 BASE-X Gigabit Ethernet – SX, LX, CX
802.3ab	1999	1000 BASE-T Gigabit Ethernet over twisted pair
802.3ac	1998	Frame size extension to 1522 bytes for VLAN tag
802.3ad	2000	Link aggregation for parallel links
802.3ae	2002	10 GBASE-T/CX4/SR/LX4/LR/SW/LW (LAN/WAN)
802.3ap	2007	Sur fond de panier au moins 1 m
802.3ba,bg, bj, bm, cd	2010 - 2018	40GBASE et 100GBASE (LAN/MAN/WAN), SDH/SONET
802.3bs	2017	200GBASE et 400GBASE (LAN/WAN)
...		

### III.3 Les normes IEEE 802.11

Il existe plusieurs normes IEEE 802.11, relatives aux réseaux locaux sans-fil WLAN ("Wireless LAN"), offrant chacune des caractéristiques différentes en termes de fréquence, de débit ou de portée du signal radio.

#### III.3.1 Méthode d'accès

- CSMA/CA, voir figure 7 et section II.4.4.



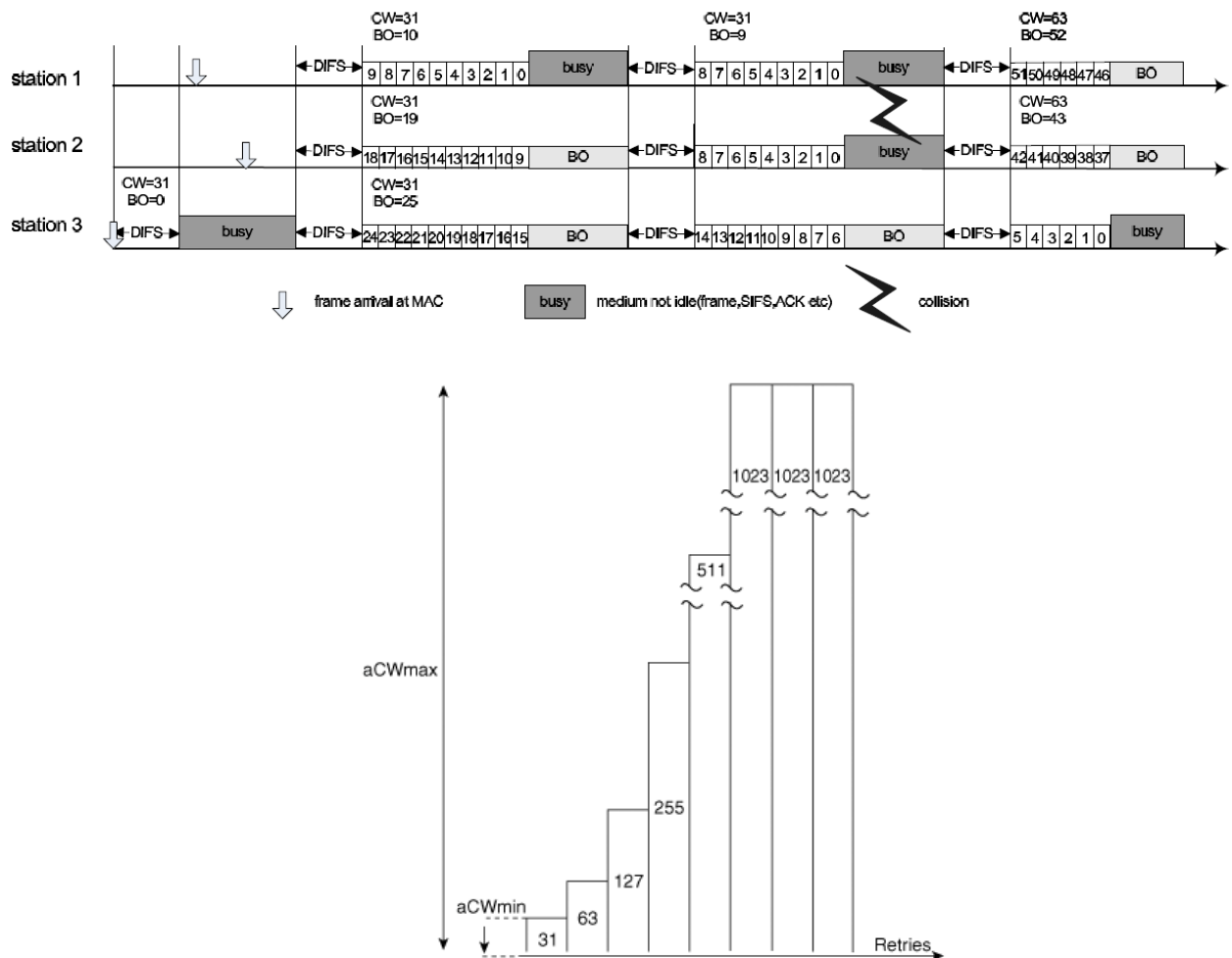


Figure 7 : la méthode CSMA/CA organigramme et illustration

- L'algorithme de back-off est appliqué dans les cas suivants :
    - ~lorsqu'une émission est retardée à cause du fait que le canal est occupé (signalé par la couche physique ou VCS),
    - ~à la suite d'une retransmission (collision),
    - ~à la suite d'une transmission ayant réussi (transmission consécutive),
- Le seul cas où cet algorithme n'est pas utilisé est lorsqu'il s'agit d'émettre une nouvelle trame et le support est resté libre pendant DIFS.
- Une variable d'état CW « Contention Window » est maintenue et initialisée à CWmin (typiquement pour FHSS/OFDM 15 et pour DSSS 31). Une taille maximale est aussi imposée notée CWmax (typiquement à 1023)
- ~Si une trame est transmise correctement (i.e., acquittée), alors  $CW = CWmin$ .

- ~Le temps de backoff BO est généré aléatoirement entre 0 et CW.
- ~Si le canal est occupé, alors BO reste inchangée (jusqu'à libération du canal).
- ~Tant que le canal est libre et  $BO \neq 0$ , alors décrémenter BO à chaque slot.
- ~Si  $BO=0$  alors l'émission peut avoir lieu.
- ~Si une transmission échoue alors  $CW = \min(CW_{max}, 2*(CW+1)-1)$  ;
- ~un nombre de retransmission maximum est prévu (paramétrable).

### **III.3.2 Autres fonctionnalités (vs. réseaux filaires)**

#### **a) Connexion au réseau et association**

Les stations écoutent les différents canaux pour localiser un point d'accès :

- une écoute passive où la station attend la réception d'une trame balise (inclut le SSID, un Timestamp et d'autres informations) émise par l'AP et
- une écoute active où la station émet des trames « Probes Request » et attend la réponse des points d'accès.

La station choisit l'AP le plus approprié, généralement celui dont le signal est de meilleure qualité. Une fois l'AP sélectionné, la station doit s'authentifier puis s'associer pour être connectée. Pour s'associer, la station doit être configurée avec le même SSID « Service Set ID » que le point d'accès (la SSID est généralement diffusée dans les trames Balise). Le diagramme d'état régissant les associations est décrit par la figure 8. Une association est identifiée par un AID « Association IDentity ». Elle peut être partagée par plusieurs APs pour faciliter la mobilité en permettant des réassociations rapides et transparentes.

La réassociation s'effectue en cas de déplacement vers un nouveau BSS, elle est invoquée par la station (au nouvel AP), elle peut être refusée. Elle se déroule comme l'association.

#### **b) Fragmentation-réassemblage**

La fragmentation réduit le taux de retransmission par des trames de plus petites tailles. Une longueur seuil, appelée `Fragmentation_Threshold`, est définie. Les fragments sont transmis de manière séquentielle, le support n'est libéré qu'une fois tous les fragments sont transmis ou lorsque la station source ne réussit pas à recevoir l'acquittement d'un fragment (figure 9).



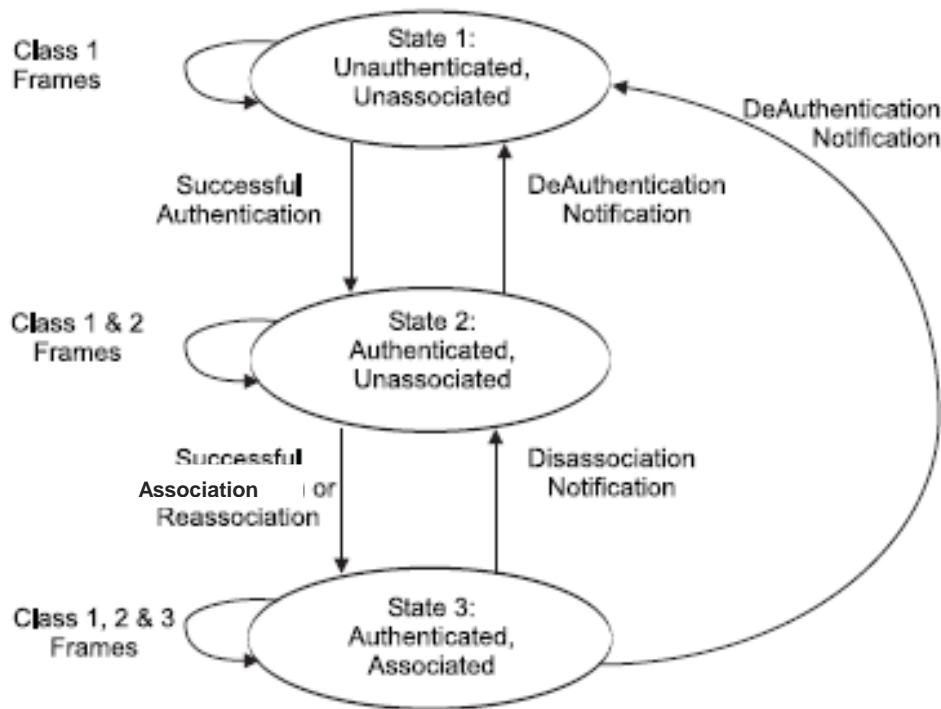


Figure 8 : diagramme d'état-transition régissant les associations

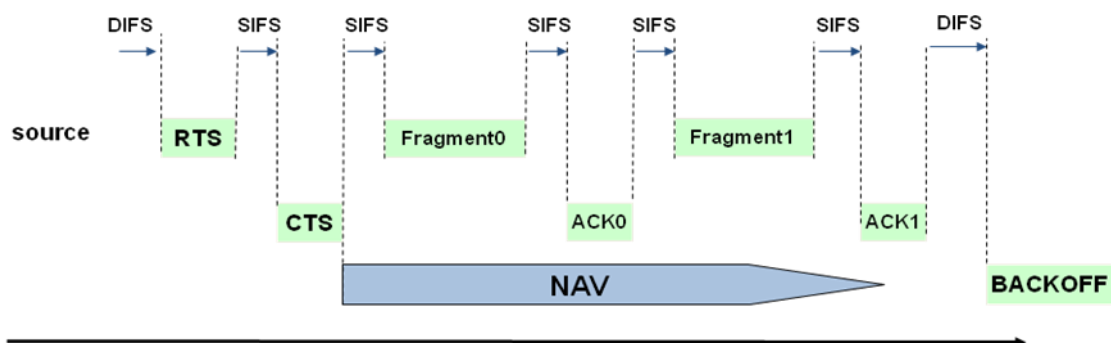


Figure 9 : exemple de transmission d'une trame fragmentation

### c) Economie d'énergie

Deux modes de fonctionnement pour les terminaux sont prévus :

- « Continuous Aware Mode », celui par défaut, le terminal est toujours allumé.
- « Power Save Polling Mode », pris en charge par l'AP. Suivant ce mode, la station désactive son dispositif sans fil régulièrement. L'AP, auquel elle est associée, met alors les trames destinées à la station dans une mémoire tampon. Les stations en veille s'activent régulièrement pour recevoir les trames dans la mémoire tampon au niveau de l'AP. A cet effet, différentes méthodes ont été proposées. Nous citons une première méthode, utilisée par « legacy », suivant laquelle, périodiquement, la station réactive le dispositif radio et attend l'arrivée de la trame de balise « Beacon » provenant de l'AP et qui peut contenir des informations TIM « Traffic Indication Map » pour trafic unicast et

DTIM « Delivery TIM » pour trafic multicat ou broadcast » indiquant la présence de trames à son intention (dans la mémoire tampon). La station utilise alors une requête PS-Poll par trame envoyée vers la station. Une deuxième méthode dite U-APSD (« Unscheduled Automatic Power Save Delivery »), utilisée pour le trafic VoIP, permet à une station de récupérer toutes les trames dans la mémoire tampon de l'AP dès que la station envoie une trame vers l'AP. Une troisième méthode consiste à ce que l'AP fixe la période de service pour l'envoi des trames dans sa mémoire tampon suivant un ordonnancement prédéterminé ce qui permet de réduire la contention S-APSD (« Scheduled APSD »).

#### **d) Sécurité**

La communication, se réalisant par onde radio, couvre une zone plus étendue qu'on ne le souhaite. Tout ce qui est transmis peut être intercepté. Pour remédier à ce problème de sécurité, l'IEEE a défini des mécanismes de chiffrement des données et d'authentification. Plusieurs protocoles de sécurisation ont été définis, dont le WEP « Wired Equivalent Privacy » et le WPA « Wi-Fi Protected Access ».

Suivant le WEP, deux modes d'authentification ont été prévus : « Open System Authentication » et « Shared Key Authentication ». L'authentification « Open System » ne requiert réellement pas d'authentification spécifique. Si aucun chiffrement n'est activé sur le réseau, tout périphérique peut écouter toutes les données qui transitent sur le réseau. L'authentification « Shared Key » exige que le chiffrement soit activé avec une même clé sur le client et l'AP. Le client doit savoir crypter un défi « text-challenge ». En plus de ces deux modes d'authentification spécifiés par le standard, certains fabricants proposent l'authentification par adresse MAC. L'AP maintient alors une liste d'adresses autorisées, le processus d'authentification continue uniquement si l'adresse du client est présente dans la liste. En utilisant le WEP, chaque terminal possède une clé secrète partagée de 40 bits et peut passer à 104 bits. Cette clé est concaténée avec un code de 24 bits, l'IV « *Initialization Vector* », qui est réinitialisé à chaque transmission. La nouvelle clé de (64 ou 128 bits, certaines implémentations sont passées à 256 bits) est placée dans un générateur de nombre aléatoire qui détermine une séquence de clés pseudo-aléatoires, qui permet de chiffrer les données. Une fois chiffrée, la trame peut être envoyée avec son IV. Pour le déchiffrement, l'IV sert à retrouver la séquence de clés qui permet de déchiffrer les données. Le chiffrement ne protège que les données de la trame et non les en-têtes. Le WEP utilise la somme de contrôle CRC-32 pour assurer l'intégrité du message.

Devant la grande vulnérabilité du WEP, le WPA (version allégée de la norme IEEE 802.11i) a été défini pour corriger les failles de sécurité du WEP. Une clé de 128 bits ou de 256 bits est utilisée et l'IV passe à 48 bits. Des protocoles d'authentification et de cryptage plus robustes sont appliqués. Le TKIP « Temporary Key Integrity Protocol » permet la génération

aléatoire de clés (dynamiques) et permet de modifier la clé de chiffrement plusieurs fois par seconde. Cependant, ce protocole n'est pas suffisamment robuste et peut lui aussi être cassé en quelques minutes. Une deuxième génération (WPA2), assez robuste, est le protocole AES-CCMP «Advanced Encryption Standard-Counter with Cipher block chaining Message authentication code Protocol» (définie dans le standard IEEE 802.11i). Deux modes de fonctionnement sont prévus : le mode PSK « *PreShared Key* » - appelé aussi mode Personnel - s'appuyant sur un secret partagé et le mode basé sur la norme 802.1x pour une authentification centralisée, une prise en charge de la gestion et de la distribution des clés (indépendante de la norme 802.11 et utilisée que ce soit pour un réseau filaire ou un réseau sans fil, il s'agit d'un protocole permettant de n'autoriser l'accès à un port réseau qu'après authentification), appelé aussi mode Entreprise. La norme 802.1x utilise un protocole d'authentification existant l'EAP « Extensible Authentication Protocol ». Dans le cas d'un réseau WiFi, l'authentification 802.1x comporte trois composants : l'authentificateur (le point d'accès), le demandeur (le client) et le serveur d'authentification (exemple, RADIUS). Le point d'accès, authentifie le client en faisant appel au serveur d'authentification suivant le protocole EAP. Ce serveur peut authentifier l'utilisateur (par mot de passe ou certificats) ou le système (par adresse MAC). Différents types d'authentification sont possibles : EAP-TLS, EAP-TTLS et PEAP « Protected EAP ». Il existe une autre authentification 802.1x : la Cisco LEAP « Cisco Light EAP », en outre Cisco a introduit la fonctionnalité CCKM « Cisco Centralized Key Management », qui permet à un point d'accès, configuré pour fournir des services WDS « Wireless Domain Services » de prendre la place du serveur d'authentification pour les opérations re-authentification de stations (qui ont changé de point d'accès). WPA2, version de la norme IEEE 802.11i certifiée par la Wi-Fi Alliance, impose la prise en charge de l'AES-CCMP. Le WPA n'est pas compatible avec les réseaux Ad Hoc. C'est l'une des raisons de l'apparition de WPA2 qui est une version améliorée de WPA et qui permet d'utiliser WPA au niveau des réseaux ad-hoc. Une nouvelle génération WPA3 est venue améliorer la sécurité WPA2 notamment contre certaines attaques (force brute) en utilisant une méthode appelée SAE « Simultaneous Authentication of Equals » celle-ci fait appel à une clé PMK « Pairwise Master Key » propre à chaque extrémité (égal qui peut être un client Wifi ou un point d'accès) et dérivée d'un mot de passe pré-partagé (PSK). A partir de la clé PMK est générée une clé de session PTK « Pairwise Transient Key ».

#### e) **Handovers et mobilité**

Le Roaming ou le Handover survient lorsqu'une station se déplace d'une cellule à une autre. Contrairement à la téléphonie mobile les Handovers en WiFi se font entre deux transmissions de données. Le standard ne fournit pas un mécanisme de handover à part entière, mais définit quelques règles (synchronisation, association, ré-association ...), ce qui a laissé le champ libre à des implémentations propriétaires. Si une station se déplace, elle cherchera le meilleur point d'accès pour s'associer avec lui, mais toute communication sera interrompue et non

reprise par le nouveau point d'accès. La borne à laquelle s'associe une station est choisie suivant des critères, tels que la puissance du signal, le taux d'erreur des paquets, la charge réseau ... Une première norme 802.11f a été élaborée afin de supporter le roaming mais elle a été retirée en février 2006 (roaming lent, non finalisée, désintéressement des acteurs). Une seconde norme a été ensuite définie : la norme 802.11r. Sans le recours à cette norme, la reconnexion prend quelques dixièmes de seconde, voir quelque secondes, ce qui ne pose pas de réels problèmes dans le cas de bon nombre d'utilisations. Mais dans le cas d'une conversation téléphonique la moindre coupure est audible. Avec la norme 802.11r, la connexion au nouveau réseau se fait avant la déconnexion, ce qui permet d'avoir des coupures de tout au plus 50 ms.

### III.3.3 Format d'une trame

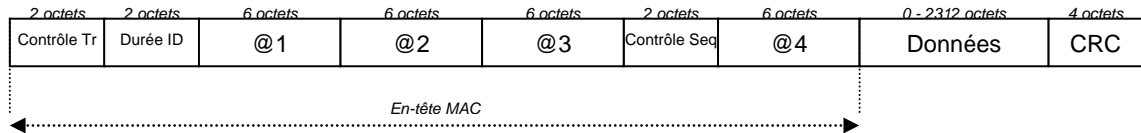
Il existe trois principaux types de trames :

- les trames de données, utilisées pour la transmission des données,
- les trames de contrôle, par exemple RTS, CTS et ACK,
- les trames de gestion, pour l'échange d'informations de gestion au niveau MAC : associations ou les désassociations d'une station avec un AP ...

Toutes les trames 802.11 sont structurées de la manière suivante :

<u>Longueur variable</u>	Préambule
<u>Longueur variable</u>	PLCP
<u>2346 octets</u>	Données MAC
4 octets	CRC

- Le **préambule** (envoyé à 1 Mb/s) comporte :
  - ~une séquence de 80 bits alternant 0 et 1 (appelée Synchronisation), utilisée par la couche physique pour sélectionner l'antenne et la synchronisation,
  - ~une séquence SFD de 16 bits (0000 1100 1011 1101), utilisée pour définir le début de la trame.
- L'en-tête **PLCP** « Physical Layer Convergence Protocol », transmis à 1, 2, 6 Mb/s selon la technique de modulation, l'entête PLCP permet de décoder la trame, elle comporte notamment :
  - ~la longueur (en octets) de mot du PLCP\_PDU, utilisé pour détecter la fin du paquet,
  - ~ la vitesse de transmission entre la carte coupleur et le point d'accès,
  - ~un champ de détection d'erreur CRC sur 16 bits
- Le format général des **données MAC** est le suivant :



~le contrôle de trame (FC : « Frame Control ») est constitué des informations suivantes :

- « *Version de protocole* » : 2 bits, version du standard 802.11.
- « *Type et Sous-type* » : ces champs, respectivement de 2 et 4 bits, définissent le type et le sous-type des trames (trames de données, des trames de services).
- « *To DS* » : 1 bit, à 1 pour toute trame envoyée par une station à destination d'un point d'accès (le Système Distribution DS).
- « *From DS* » : 1 bit, à 1 lorsque la trame provient du DS. Lorsque les deux champs To et From sont positionnés à zéro il s'agit d'une communication directe entre deux stations (mode ad hoc).
- « *More Fragments* » : 1 bit, lorsqu'il est à 1 il reste des fragments à transmettre.
- « *Retry* » : 1 bit, lorsqu'il est à 1 spécifie que le fragment en cours est une retransmission d'un fragment précédemment envoyé (déjà perdu).
- « *Power Management* » : 1bit, lorsqu'il est à 1, la station ayant envoyé ce fragment entre en mode de gestion d'énergie (elle n'écoute pas à tout moment et peut interroger un AP pour récupérer des trames en attente).
- « *More Data* » : 1 bit, en mode de gestion d'énergie, il est utilisé par un AP pour spécifier à une station que des trames supplémentaires sont stockées en attente.
- « *WEP* » : 1 bit, indique que l'algorithme de chiffrement WEP a été utilisé pour chiffrer le corps de la trame.
- « *Order* » : indique que la trame a été envoyée en utilisant la classe de service strictement ordonnée « *Strictly-Ordered service class* ». La trame doit être traitée en respectant entre les trames unicast et multicast.

~Durée / ID : indique la durée d'utilisation du canal de transmission (estimé par l'émetteur), il permet la mise à jour du NAV. Il est aussi utilisé comme identificateur de station pour les trames de polling en mode d'économie d'énergie.

~Adresse 1 : adresse du récepteur. Si ToDS est à 1, c'est l'adresse du AP, sinon, c'est l'adresse de la station.

~Adresse 2 : adresse de l'émetteur. Si FromDS est à 1, c'est l'adresse du Point d'Accès, sinon, c'est l'adresse de la station émettrice.

~Adresse 3 : adresse de l'émetteur original quand le champ FromDS est à 1. Sinon, et si ToDS est à 1, Adresse 3 est l'adresse destination.

~Contrôle de séquence : ce champ permet de distinguer les divers fragments d'une même trame. Il est composé de deux sous-champs permettant de réordonner les

fragments : le numéro de fragment, le numéro de séquence (identique pour les fragments d'une même trame)

~Adresse 4 : utilisé quand le système de distribution sans fil est utilisé et qu'une trame est transmise d'un AP à un autre. Dans ce cas, ToDS et FromDS sont tous deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire. Adresse 4 indique l'émetteur original (adresse 3 indique la destination finale et adresse).

~Données : y compris les entêtes associés au cryptage.

~CRC : une somme de contrôle servant à vérifier l'intégrité de la trame.

Le tableau suivant résume la signification de chaque champ d'adresse selon FromDS et ToDs (le BSSID identifie le BSS, en mode infrastructure il correspond à l'adresse MAC de l'interface du point d'accès ayant créé le BSS) :

ToDS	FromDS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

### III.3.4 Primitives de services

Les primitives de service sont comparables à ceux de la couche MAC IEEE 802.3.

- MA-UNITDATA.request(*adresse\_source*, *adresse\_destination*, *information de routage*, *MA\_SDU*, *priorité*, *Classe\_de\_service*)
- MA-UNITDATA.indication(*adresse\_source*, *adresse\_destination*, *information de routage*, *MA\_SDU*, *status*, *priorité*, *Classe\_de\_service*)
- MA-UNITDATA-STATUS.indication(*adresse\_source*, *adresse\_destination*, *status*, *priorité\_fournie*, *Classe\_de\_service\_fournie*)

Avec :

- *information\_de\_routage* non utilisé (nul),
- *status* : coté émetteur peut être succès, échec avec nombre de tentatives limite atteint, coté récepteur, longueur trop grande, priorité/service non supportée, échec contrôle de sécurité ....
- *priorité* : « Contention » DCF, « Contention Free » PCF.
- *Classe\_de\_service* : « Reorderable » ou « StrictlyOrdered » (entre les trames unicast et multicast).

### III.3.5 Principales caractéristiques physiques

La couche physique, chargée de véhiculer des bits, utilise l'onde hertzienne. Deux sous-couches ont été définies :

- PLCP « Physical Layer Convergence Protocol », elle écoute le support et indique ainsi à la couche MAC via un CCA « Clear Channel Assessment » si le support de transmission est libre ou non
- PMD « Physical Medium Dependur », s'occupe de l'encodage des données.

Comme nous l'avons déjà décrit dans le chapitre précédent, la norme de base spécifie différents modes de transmission : FHSS « Frequency Hopping Spread Spectrum », DSSS « Direct Sequence Spread Spectrum », OFDM « Orthogonal Frequency Division Multiplexing ». En plus elle prévoit le mode IR Infra Rouge pour la communication entre stations proches. Le tableau suivant résume les propriétés de ces différents modes.

En pratique la portée dépend de certains paramètres physiques, comme la puissance d'émission, spécifiés par la réglementation, mais elle dépend aussi de la qualité des produits et de l'environnement considéré (nature des obstacles). Elle est de quelques dizaines de mètres à l'intérieur d'un bâtiment, à quelques centaines de mètres à l'extérieur. La portée augmente en réduisant le débit. Si la liaison n'est pas satisfaisante, le débit nominal peut se replier sur des débits inférieurs (cf. chapitre IV).

	802.11	802.11a	802.11b	802.11g	...
Bande (Ghz)	2,4	5	2,4	2,4	
Débit Max. (Mb/s)	2	54	11	54	
Modulation	FHSS/DSSS	OFDM	DSSS	DSSS / OFDM	

### Exercice 1

On considère un réseau local Ethernet. La retransmission en cas de collision est effectuée selon l'algorithme du retard exponentiel binaire BEB. Ce réseau gère les transmissions entre 4 stations A, B, C et D. Dans ce problème on utilise comme mesure de temps le "time slot" qui est le temps d'allée-retour. Les délais d'espacement inter-trames ainsi que les durées de détection de voie libre sont négligés. Le temps de détection de collision est égal à 1 slot.

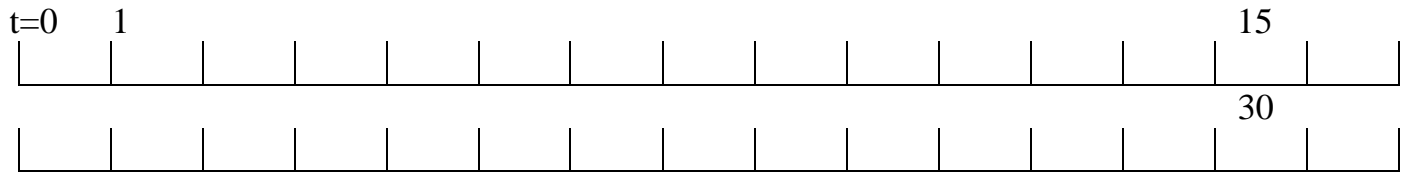
A l'instant  $t = 0$  la station A acquiert la voie et commence à transmettre un message. A l'instant  $t = 5$  les stations B, C, et D reçoivent une demande de transmission d'une trame. Puis, pendant toute la durée considérée dans l'exercice aucune autre demande de transmission n'est soumise aux stations. Tous ces messages sont de taille fixe et la durée de leur transmission est égale à **2** slots.

Dans l'exemple on considèrera que la fonction de tirage aléatoire rend successivement pour chaque station les valeurs données par le tableau suivant :

	<b>B</b>	<b>C</b>	<b>D</b>
<b>1er tirage</b>	1	1	1
<b>2ème tirage</b>	3	3	2
<b>3ème tirage</b>	2	5	4

1) Compléter le diagramme suivant en indiquant pour chaque slot l'état de la voie.

Un slot occupé par la transmission d'un message correctement émis par la station A est représenté par "A", un slot occupé par une collision est représenté par "X". Un slot correspondant à une absence de transmission est représenté par "—".



2) Calculer le taux d'utilisation de la voie sur la période allant de  $t = 0$  à la fin de la transmission du dernier message.

3) A l'instant  $t=20$  B et C envoient chacun une nouvelle trame ce qui provoque une collision, à quel intervalle devrait appartenir la valeur aléatoire générée par B ou C ?



## IV. Déploiement des réseaux locaux

Ce chapitre présente les composants des réseaux locaux Ethernet et WiFi. L'organisation d'un plan de câblage d'un réseau local est aussi abordée.

### IV.1 Ethernet

#### IV.1.1 Ethernet II (DIX) vs Ethernet IEEE 802.3

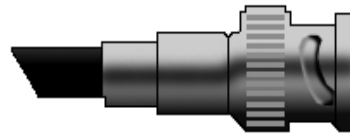
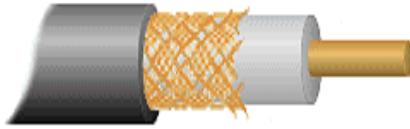
Le réseau Ethernet est issu des travaux de recherches lancés au début des années 70 par Xérox sur les techniques d'accès aléatoire pour les LAN. En 1980 la première version 2 (ou DIX) a été réalisée en collaboration avec Digital et Intel. Depuis le réseau Ethernet a connu plusieurs évolutions. En 1985, l'IEEE reprend les spécifications Ethernet et elle les formule dans la publication IEEE 802.3. Certaines modifications ont été introduites notamment au niveau du câblage. Au niveau physique, les réseaux Ethernet actuels se conforment aux normes IEEE 802.3. Les différences au niveau MAC seront étudiées dans le chapitre V.

#### IV.1.2 Composants d'un réseau Ethernet 802.3

- média et connectique :

- 10 BROAD 36 : câble coaxiale CATV (RG6), semi-rigide, large bande, 10 Mb/s, topologie en bus, longueur maximale sans répétition 3600 m, nombre maximal de nœuds par segment 1024.
  - 10 BASE 5 (Ethernet de base): câble coaxial 50  $\Omega$  (le blindage composé de tresses et d'écrans) ; rayon de courbure 25 cm ; vitesse de propagation =  $0.77 \cdot c = 2,31 \cdot 10^8$  m/s ; temps bit = 0,1  $\mu$ s (1/débit) ; longueur = multiples impaires de 23,4 m (pour que les réflexions ne soient pas en phase. Considérer la moitié de la longueur d'onde à 5 Mhz :  $23,4 \text{ m} \cong (2,31 \cdot 10^8) / (2 \cdot 5 \cdot 10^6)$ ); connectique de type N (avec filetage) ; topologie en bus ; longueur maximale d'un segment 500 m ; le nombre maximal de nœuds par segment 100, le nombre maximal de répéteurs 4. transmission en bande de base (Manchester) ; 10 Mb/s ;
  - -10 BASE 2 (Cheapernet) : câble coaxial 50  $\Omega$  (souple le blindage est composé de tresses, le câble est en fils multi-brins) ; rayon de courbure 5 cm ; vitesse de propagation =  $0.65 \cdot c = 1,95 \cdot 10^8$  m/s ; temps bit = 0,1  $\mu$ s (1/débit) ; connectique de type BNC (Bayonnet-Neil-Concelman); transmission en bande de base (Manchester) ; topologie en bus ; longueur maximale d'un segment 185 m ; longueur minimale entre nœud 0.5 m ;

nombre maximal de nœuds par segment 30, nombre maximal de répéteurs 4\* ; 10 Mb/s.



- 10/100/1000 BASE T (Starlan) : paire torsadée, différentes catégories de câbles (voir chapitre II) ; connectique RJ45 (8 broches dont 2 pour l'émission et deux pour la réception). topologie en étoile, la longueur recommandée d'un câble est de 100 m.

Selon la norme TIA-568B, le code couleur suivant est appliqué (un autre code couleur est utilisé pour la norme TIA-568A, où le vert et l'orangé sont permutés par rapport à la norme TIA-568B)

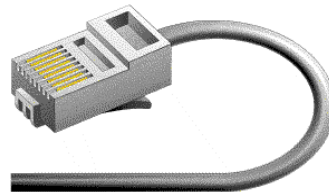
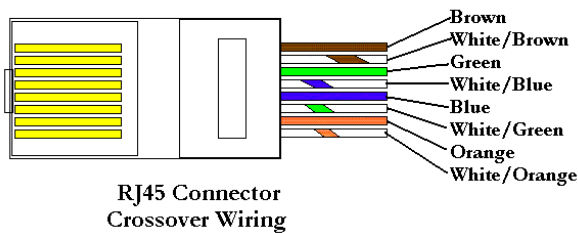
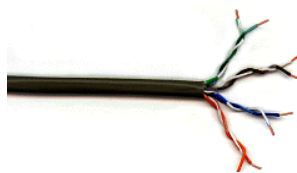
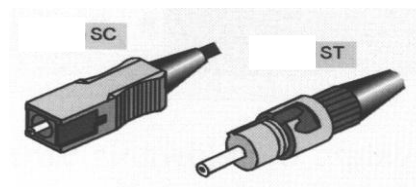
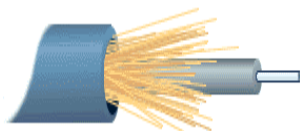


Schéma d'un câble RJ45 croisé pour à 10/100/1000 Tx / 2 paires (entre parenthèses les désignations utilisées pour 1000 BASE T / 4paires)

Nom	NCI 1	NCI 2	Nom
<b>TX+</b> (BI_DA+)	<b>1</b>	<b>3</b>	<b>RX+</b> (BI_DB+)
<b>TX-</b> (BI_DA-)	<b>2</b>	<b>6</b>	<b>RX-</b> (BI_DB-)
<b>RX+</b> (BI_DB+)	<b>3</b>	<b>1</b>	<b>TX+</b> (BI_DA+)
- (BI_DC+)	4	7	- (BI_DD+)
- (BI_DC-)	5	8	- (BI_DD-)
<b>RX-</b> (BI_DB-)	<b>6</b>	<b>2</b>	<b>TX-</b> (BI_DA-)
- (BI_DD+)	7	4	- (BI_DC+)
- (BI_DD-)	8	5	- (BI_DC-)

Le PoE (Power over Ethernet), décrit par les normes IEEE 802.3af/at, supporte l'alimentation électrique à travers le câble réseau en faisant appel aux deux paires non utilisées.

- 10 BASE FP (Fiber Passive) : fibre optique, 10 Mb/s, point à point, topologie en étoile, longueur maximale d'un câble 1 Km, HUB passif.
- 10 BASE FL (Fiber Link) : fibre optique, 10 Mb/s, point à point, topologie en étoile, longueur maximale d'un câble 2 Km.
- 10 BASE FB (Fiber Backbone) : fibre optique, 10 Mb/s, point à point, longueur maximale d'un câble 2 Km (« Inter Repeater Link »).



- **TRANSCEIVER** ("TRANSMitter reCEIVER") et **convertisseurs de média**.  
Un transceiver ("transmitter receiver"), appelé aussi MAU ("Medium Attachment Unit"), est l'élément qui se connecte directement au média et qui se charge de l'émission et de la réception des signaux sur le support de transmission. Il détecte les collisions par comparaison entre les signaux émis et les signaux reçus pendant le RTD, le processus est analogique. Le transceiver assure aussi certaines fonctions particulières comme la protection « jabber » contre les trames trop longues. Dans ces deux dernier cas, il active le signal de présence de collision ou de trame tronquée « Signal Quality Error » ou « Heart Beat »<sup>1</sup>. Dans le cas de l'Ethernet de base (10 BASE 5), un transceiver à piquage est utilisé où une aiguille est introduite dans le câble et mise en contact avec le conducteur central. Le transceiver possède une ou plusieurs prises DB15 (15 broches) sur lesquelles sont branchés les câbles AUI ("Attachment Unit Interface"). Dans le cas du Cheapernet (10 BASE 2), le transceiver est relié au média à travers un T. Il est souvent intégré dans la carte coupleur. Dans le cas contraire, il est relié au coupleur par une prise DB15 (alimentation, collision, émission, réception,...).

---

<sup>1</sup> Le test SQE : Le signal SQE peut être utilisé en tant que test, on l'appelle alors SQE(T). Il sert à vérifier la connexion entre la station et le transceiver. Il est émis uniquement vers la station et non vers le réseau.. Le SQE(T) est appliqué entre chaque trame et a reçu pour cette raison le nom de « Heart Beat » (battement de cœur). Il peut être activé ou désactivé par un interrupteur. Il ne faut surtout pas l'activer si la station n'en connaît pas la signification. Il pourrait être interprété comme un SQE standard et faire croire à la station qu'il y a un taux anormal de collisions.

Les transceivers offrent la possibilité de changer de média sans changer la carte coupleur. Pour les réseaux Gigabit, il est possible de changer de média moyennant un adaptateur intégré appelé GBIC (Gigabit Interface Converter). Un GBIC est une interface interchangeable à chaud permettant de convertir le signal. IL existe aussi des convertisseurs de média, permettant de se connecter à travers un port RJ45 à un port SC.



- **Câble de transceiver** : également appelé Attachment Unit Interface (AUI), ou câble de descente (drop cable), il relie le transceiver au coupleur, sa longueur maximum de 50 m, utilise un connecteur 15 pins, le câble est constitué de 4 ou 5 paires torsadées :
  1. une paire pour l'alimentation
  2. une paire pour les signaux de données en entrées
  3. une paire pour les signaux de données en sortie
  4. une paire pour les signaux de contrôle en entrées: transceiver prêt à émettre, transceiver non prêt à émettre, erreur de qualité de signal (SQE) émis sur détection de collision ou trame tronquée (jabber)
  5. une paire optionnelle pour les signaux de contrôle en sortie (coupleur --> transceiver) permettant de commander le transceiver : entrer en mode monitor, passer en mode normal ...
- **Fan out** ou multiplicateur d'accès : ce dispositif permet de connecter plusieurs nœuds à un même transceiver via des câbles AUI (pour 10 BASE 5).
- **Répéteur** : il permet de relier deux segments. Le nombre de répéteurs est limité selon la norme utilisée.

Un répéteur est particulièrement utile pour relier un réseau Ethernet de base à un réseau Cheapernet. Il existe des répéteurs distants qui permettent de relier deux segments éloignés. Ces répéteurs sont formés de deux répéteurs reliés par un câble couvrant la distance en question.



BNC/BNC



AUI/AUI

- **Carte coupleur** (NIC : « Network Interface Card ») : chargé de contrôler les communications en particulier les fonctions de la couche physique du modèle OSI et de la sous-couche MAC. Il existe des coupleurs dits intelligents qui gèrent des fonctions de niveaux supérieurs (LLC et plus). La carte coupleur est montée sur le bus de la machine (PCI 32/64 bits, ISA/EISA, CardBus/Card PCMCIA ...). Elle peut être munie de plusieurs ports (BNC, AUI-DB15, RJ45). Une carte réseau est généralement capable de réaliser *l'auto-négociation* du débit 10/100/1000 Mb/s et du mode « Full » ou « Half » duplex. Suivant la norme IEEE 802.3x une carte peut aussi se soumettre à un contrôle de flux (lorsqu'elle est raccordée à un commutateur mettant en œuvre ce contrôle). Certaines cartes offrent la fonction WOL (Wake-On-LAN) : l'ordinateur peut être mis ON/OFF à distance. Pour disposer d'un débit plus important, il est possible de trouver des cartes qui réalisent l'agrégation de liens (IEEE 802.3ad).



A l'émission, les contrôles de transmission effectués par la carte coupleur sont :

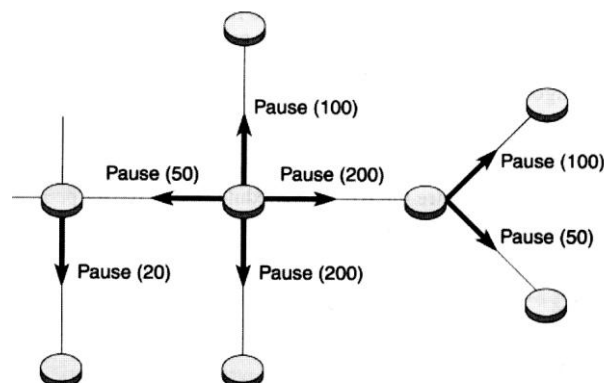
- construction de la trame,
- attente de la libération du canal, l'émission est initialisée après un délai/espace inter-trame minimum (IFG : "Inter-Frame Gap") de 9,6  $\mu$ s pour l'Ethernet, de 960 ns pour le Fast Ethernet et de 96 ns pour le Gigabit Ethernet. Il permet de déceler le repos du signal et de donner la possibilité aux interfaces réseaux de se préparer et d'émettre,
- Surveillance du canal, en appliquant la méthode d'accès CSMA/CD.

A la réception, les actions suivantes sont effectuées :

- détection de l'arrivée d'une trame,
- réception bit par bit jusqu'au repos du signal,
- vérification que la taille de la trame n'est pas courte ("runt"),
- comparaison des adresses du nœud et de destination, s'ils sont égaux la trame est retenue pour être délivrée à la couche supérieure,
- vérification de l'alignement et du FCS,
- vérification que la taille de la trame n'est pas longue ("jabber"),

- **Hub** : il a été introduit dans le réseau Starlan (10 BASE T) pour réaliser une topologie en étoile dont les nœuds sont les Hubs (d'où le nom en anglais). Un Hub récupère le signal par une entrée et duplique ce signal sur les sorties. Un Hub est actif, il ré-amplifié (répété) le signal. La possibilité d'empiler les Hubs à travers des ports appropriés permet de remédier en partie aux contraintes liées au nombre de segments qu'on peut cascader.
- **Commutateur** (Switch) permet d'interconnecter des stations, des HUBs ou des segments Ethernet. Pour augmenter le débit on peut passer à la commutation Ethernet duplex integrale FDSE (Full Duplex Switched Ethernet). La commutation Ethernet abandonne le principe du médium partagé Plusieurs transmissions peuvent avoir lieu en même temps. Deux techniques de commutation sont proposées par les constructeurs :
  - « Cut-Through » ou « on the fly »: la retransmission peut avoir lieu dès le décodage de l'adresse du destinataire. La réception et la transmission d'une trame se fait en même temps.
    - Temps de transit minimal
    - Le contrôle d'erreurs n'est pas possible
    - La conversion de vitesse n'est pas possible
  - « Store and Forward » : réception de la trame complète avant de pouvoir la retransmettre.
    - Temps de latence plus importante (de l'ordre de 50 ms)
    - Permet de filtrer les trames erronées
    - Nécessite une mémoire tampon de grande taille
  - « Adaptive Error Free » : combine de techniques précédentes. Le commutateur fonctionne en « Cut-Through » tant que le taux d'erreur reste acceptable et change en « Store and Forward » sinon.
  - « Fragment Free » : le « cut-through » est appliqué après lecture de 64 octets ce qui permet d'éviter les erreurs « runt ». Cette technique est appliquée lorsque le port source est HD et n'a aucun intérêt s'il est HD.

Un commutateur implémentant la norme IEEE 802.3x peut réaliser un contrôle de flux (en full duplex). Ce contrôle est déconseillé si la QoS est active.





L'aiguillage des trames, par auto apprentissage, se fait suivant le principe du pontage transparent (« transparent bridging ») et en ayant recours, si nécessaire, au protocole « Spanning Tree » (IEEE 802.1d). Les techniques de pontage seront étudiées au chapitre V.

Pour augmenter le débit entre deux commutateurs connectés entre eux (« trunk links »), plusieurs ports Ethernet peuvent être utilisés (IEEE 802.1ad).

Un commutateur peut être de niveau 2 (comparable à un pont) ou de niveau 3 (peut fonctionner en tant que routeur).

*Format d'équipement concentrateur (HUB / Commutateur)*

1. "Stand alone"

*Entrée de gamme*

*Nombre limité de ports (8, 16, 24 ou 32)*

2. Empilable "Stackable"

*Possibilité de les relier via des câbles propriétaires*

*Le tout représente une seule unité logique*

*Equipements d'un même constructeur (5-8) !*

*Adapté lorsque le nombre de postes est inférieur à 100*

3. Châssis (modulaire)

*Possibilité d'insérer différentes cartes (hub/switch) Ethernet (ou autre Token-Ring, FDDI, ATM ...) fonctionnant à différents débits, sur des segments séparés*

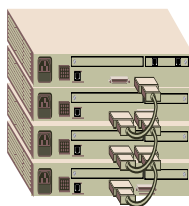
*Nombre de cartes limité par le nombre de slots*

*Bus du fond de panier peut supporter jusqu'à plusieurs Gb/s*

*Adapté lorsque le nombre de postes est supérieur à 100*



"Stand alone"



Empilable "Stackable"



Châssis

Les commutateurs peuvent (en option) permettre de définir des réseaux locaux virtuels (VLAN : « Virtual LAN »). Les VLANs sont des sous-réseaux logiques définis sur un même réseau physique. Il est ainsi possible de scinder un réseau déjà câblé en des groupes selon des critères logiques :

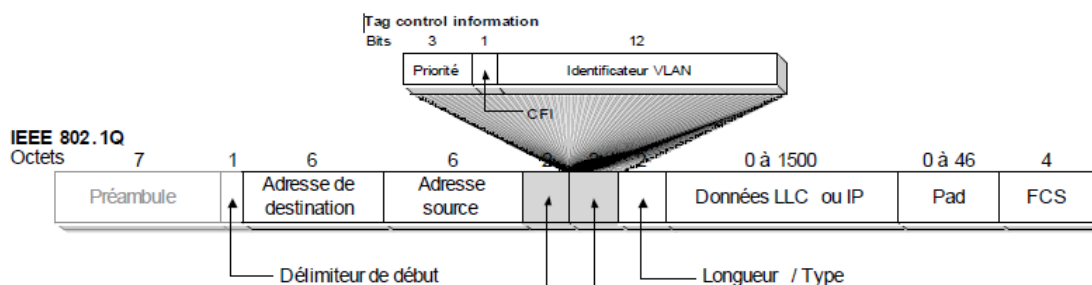
- délimiter les diffusions qui sollicitent les couches supérieures pour une meilleure gestion du trafic,
- séparer les ressources selon des critères d'appartenance, de partage ou de sécurité (protection du backbone).

La structuration en VLANs permet ainsi de s'abstraire de la disposition physique des stations lors de la définition des sous réseaux (réseaux capillaires). Elle facilite ainsi le contrôle des domaines de diffusion, la mobilité des utilisateurs et donc l'optimisation du réseau et les contrôles de sécurité.

Un VLAN est constitué d'un sous-ensemble de stations reliées par un réseau Ethernet virtuel. Une trame envoyée sur un VLAN n'est visible que par des stations qui appartiennent au même VLAN. Il est aussi possible de définir des stations appartenant à la fois à plusieurs VLANs. A l'intérieur d'un même VLAN, le commutateur réalise des opérations de pontage. La communication entre VLANs se fait grâce à des routeurs. Différents critères sont utilisés pour le regroupement des stations en VLAN : la définition de groupe d'adresses MAC, la définition de groupe de ports physiques au niveau des commutateurs ou encore le regroupement par protocoles.

Les Normes 802.1p et 802.1q définissent respectivement des extensions pour :

- La priorité au niveau MAC, qu'on appelle Classe de Service ou (CoS)
- L'interopérabilité des réseaux locaux commutés (Virtual Bridged Local Area Networks): un VLAN peut s'étendre sur plusieurs commutateurs. De ce fait, les liens « trunk » entre commutateurs véhiculent des trames qui s'apparentent à différents VLANs. La méthode du « tagging » est alors utilisée pour véhiculer l'identificateur du VLAN. Le commutateur d'accès marque la trame avec le VLAN d'origine grâce à un identificateur (sur 4 octets) qui est supprimé par le commutateur auquel est raccordé le destinataire. Cet identificateur permet à un commutateur non source de déterminer le port de sortie.





### IV.1.3 Composition d'un réseau Ethernet multi-segments

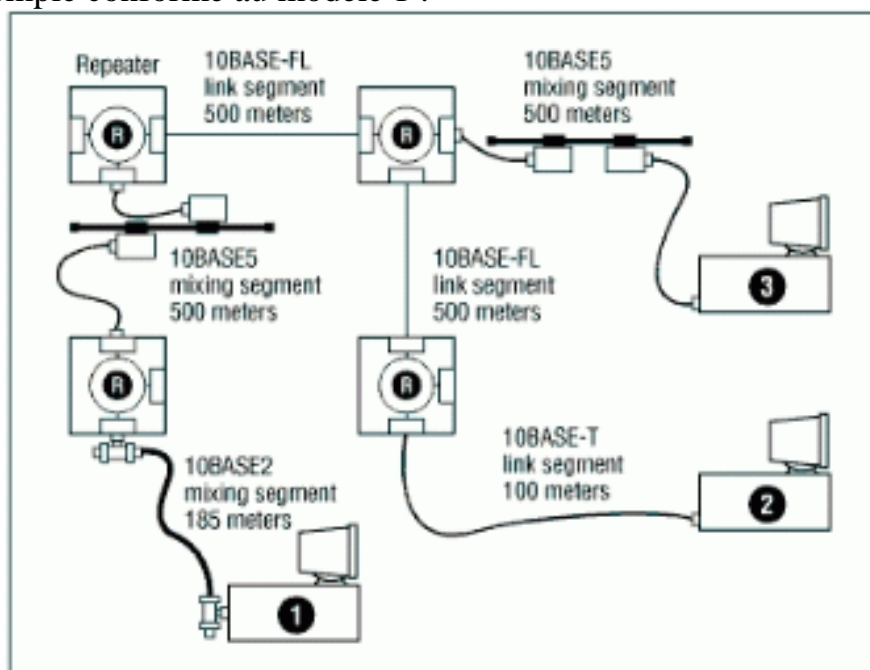
Il existe deux modèles pour pouvoir mettre en place un réseau Ethernet comportant plusieurs segments. Ces modèles garantissent que le diamètre du domaine de collision ne dépasse pas la limite autorisée et permettent de respecter la contrainte de délai inter-trame minimal (le passage à travers un répéteur risque de réduire le délai inter-trame particulièrement à cause de pertes au niveau des préambules de deux trames successives avec un nombre de bits perdus plus important pour la première trame puis restauration des préambules).

#### Modèle 1 : Règles de configuration

Le réseau doit respecter certaines règles de configuration :

- les interconnexions sont réalisées moyennant des répéteurs
- un chemin entre deux stations peut comporter cinq segments tout au plus et donc quatre répéteurs (y compris les transceivers et câbles AUI respectifs), deux transceivers et deux câbles AUI.
- les câbles AUI ne doivent pas dépasser 25m (soit 50m pour les deux câbles) pour les médias 10Base-FP et 10Base-FL.
- Si un chemin de transmission comporte cinq segments, deux de ces segments au moins doivent être de liaison,
- Si un chemin de transmission comporte cinq segments, tout segment FOIRL, 10Base-FB ou 10Base-FL ne peut dépasser 500 m alors qu'un segment 10BASE FP ne peut dépasser 300 m.
- Si un chemin de transmission comporte quatre segments, tout segment FOIRL, 10Base-FB ou 10Base-FL ne peut dépasser 1000 m alors qu'un segment 10Base-FP ne peut dépasser 700 m. Il n'existe pas de contrainte d'utilisation de segments de liaison.

Exemple conforme au modèle 1 :

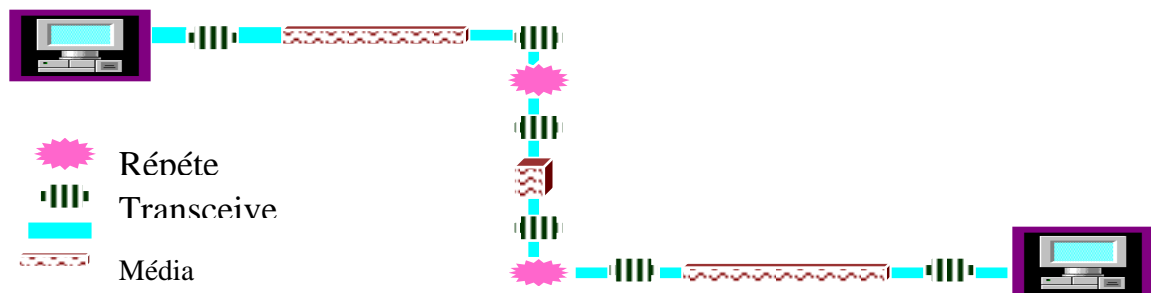


### Modèle 2 du délai d'un chemin :

Un autre modèle de l'IEEE, pour les configurations complexes, comprend un ensemble de règles de calcul permettant de calculer le délai d'aller-retour (RTD: "round-trip Delay") entre deux stations. Un autre ensemble de règles doit aussi être vérifié, il est relatif au délai inter-trame qui, s'il est en dessous de 96 temps bit, risque de créer des « overrun » à la réception. Cet ensemble de règles n'est pas illustré dans la suite. Ces deux ensembles de règles permettent ainsi de vérifier le bon fonctionnement d'un réseau.

Rappel : la spécification IEEE stipule que toute station émettrice doit être notifiée d'une éventuelle collision durant les 512 premiers bits de l'émission impliquant que le RTD (Round Trip signal Delay) ne peut excéder 512 temps bit quels que soient les médias utilisés dans la configuration.

De manière à faciliter le calcul du RTD dans un environnement multi-média, le modèle définit les segments gauche, droit et intermédiaire (un ou plusieurs) :



En fonction du type de média composant le chemin entre deux stations, l'IEEE fournit les délais induits :

Type de segment	long. Max	Segm. Base	gauche Max	Segm. Base	interm. Max	Segm. Base	droit Max	Délai / mètre
10Base5	500	11.75	55.05	46.5	89.8	169.5	212.8	0.0866
10Base2	185	11.75	30.73	46.5	65.48	169.5	188.48	0.1026
FOIRL	1000	7.75	107.75	29	129	152	252	0.1
10BaseT	100	15.25	26.55	42	53.3	165	176.3	0.113
10BaseFP	1000	11.25	111.25	61	161	183.5	284	0.1
10BaseFB	2000	-	-	24	224	-	-	0.1
10BaseFL	2000	12.25	212.25	33.5	233.5	156.5	356.5	0.1
Excès AUI	48	0	4.88	0	4.88	0	4.88	0.1026

Où :

Base = délai min. (transit de transceiver, répéteur, câble AUI de 2m, collision) pour le média utilisé

Délai / mètre = temps de traversée aller-retour pour un mètre de média utilisé. Tous les délais sont exprimés en temps bit.

Le calcul du délai d'un chemin se fait de la façon suivante :

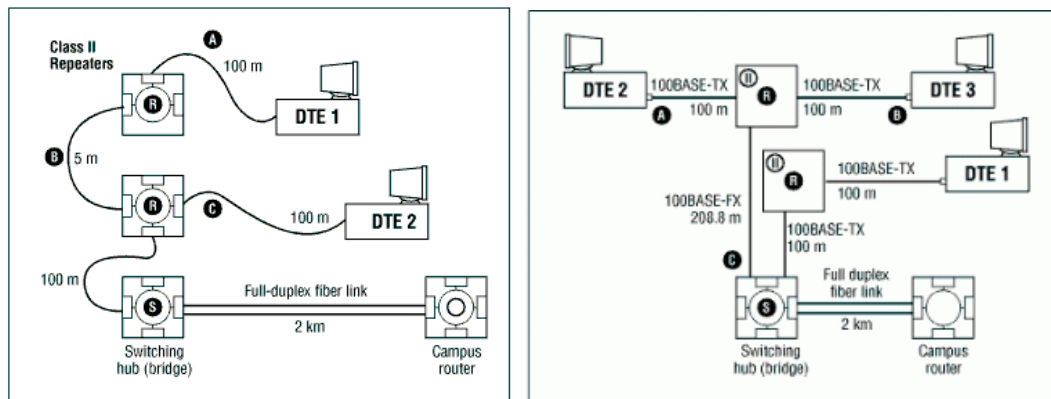
- Le délai du chemin entre deux stations est décomposé en délais de segments ou SDV « Segment Delay Value » composant le chemin. Pour un segment donné,  
$$SDV = Base + (longueur \text{ du segment} * RTD / \text{mètre})$$
- Si les segments gauche et droit sont de différents types, effectuer le calcul à nouveau en inversant la gauche et la droite et retenir le délai le plus long,
- Si les câbles AUI dépassent 2 m, rajouter le délai en excès,
- Ajouter une marge de 5 temps bit,

Si le délai ainsi obtenu est  $\leq$  à 575 temps bit, le chemin est valide. Effectuer cette procédure entre toutes les extrémités du réseau.

Les contraintes du réseau Fast Ethernet sont différentes étant donné que le débit est 10 fois plus élevé et qu'en conséquence le délai de propagation devrait être réduit du même facteur (5,12  $\mu$ s) au lieu de 51,2  $\mu$ s). Un réseau Fast Ethernet est limité à deux répéteurs et n'utilise que des segments de liaison. Le domaine de collision est limité à 205 m avec du câble UTP. Dans le cas général, la limite de distance dépend du type de répéteur. Deux classes de répéteurs sont prévues: Class I et Class II. Pour les répéteurs de Class I un seul saut de répéteur est permis. Pour les répéteurs de Class II, tout au plus deux sauts de répéteurs sont permis.

	<b>T</b>	<b>FX</b>	<b>T et FX</b>
<b>1 segment</b>	100 m	412 m	
<b>2 segments (1 répéteur Class I)</b>	200 m	272 m	100+160,8 m
<b>2 segments (1 répéteur Class II)</b>	200 m	320 m	100+208 m
<b>3 segments (2 répéteurs Class II)</b>	205 m	228 m	105+111.2 m

Alors qu'un segment en paire torsadée ne peut pas dépasser 100 m un segment en fibre optique peut aller jusqu'à 412 m. La longueur d'un segment en fibre optique entre deux commutateurs en full-duplex peut atteindre 2000 m. Les deux figures suivantes décrivent deux exemples de configuration Fast Ethernet :



Il existe aussi un modèle basé sur le calcul du RTD pour la validation de configurations plus complexes de réseaux Fast Ethernet. A cet effet, le tableau suivant peut être utilisé.

Component	RTD / mètre (temps-bit)	RTD Maximum
Deux DTEs TX/FX		100
Deux DTEs T4		138
Un DTE T4 et un DTE TX/FX		127
Catégorie 3 / 4	1.14	114 (100 m)
Catégorie 5	1.112	111.2 (100 m)
STP	1.112	111.2 (100 m)
Fibre Optique	1.0	412 (412 m)
Répéteur Classe I		140
Répéteur Classe II tous les ports TX/FX		92
Répéteur classe II avec des ports T4		67

Les constructeurs peuvent aussi fournir des tableaux plus précis relatifs à l'estimation des délais sur les câbles utilisés. Il est recommandé de rajouter une marge de 4 temps-bits au délai total qui doit être inférieur ou égal à 512 temps-bits. Remarquons aussi que ce deuxième modèle de validation ne prévoit pas le calcul du rétrécissement du délai inter-trame étant donné que le nombre de répéteur est limité.

Pour le réseau Gigabit et suivant un premier modèle de validation, le nombre de répéteurs est limité à 1 et la longueur d'un segment est limité selon le type du média et ne dépasse pas les 316 mètres. Le tableau suivant précise la longueur maximale d'un domaine de collision.

	Cat 5 UTP	CX	SX/LX	Cat 5 et F.O	CX et SX/LX
<b>1 segment</b>	100	25	316		
<b>1 répéteur</b>	200	50	220	210	220

Dans le cas d'une liaison full-duplex et en utilisant la fibre optique, il est possible d'atteindre des longueurs plus importantes comme le montre le tableau suivant.

Nom	Type	Longueur max segment	Remarques
<b>1000Base-SX</b>	2 fibres optiques	220-550m	Multimode
<b>1000Base-LX</b>	2 fibres optiques	550-5000m	Multimode - Monomode

Il est aussi possible d'utiliser un second modèle basé sur le calcul du RTD. A cet effet le tableau suivant peut être utilisé.

	RTD / mètre (temps-bit)	RTD Maximum
Deux ETSDs		864
Segment Catégorie 5 UTP	11.12	1112 (100 m)
Segment CX	10.10	253 (25 m)
Segment optique	10.10	1111 (110 m)
Répéteur		976

Les constructeurs de câbles peuvent fournir des tableaux plus précis selon le câble. Il est recommandé de rajouter une marge de 32 temps-bits au total (généralement comprise entre 0 et 40) qui doit être inférieur ou égal à 4096 temps-bits.

## IV.2 WiFi

### IV.2.1 Composants d'un réseau WiFi

- **Cartes PCI / PCMCIA/ USB** : PCI pour des ordinateurs de bureau et PCMCIA pour des ordinateurs portables. Il est aussi possible de raccorder la carte à travers un port USB.



Carte PCI



Carte PCMCIA

Wireless 2.4GHz (802.11b)  
USB Adapter  
DWL-122

*Easy to connect and share files  
over your wireless network*



- **Antennes** : il existe principalement 2 modèles d'antennes :
  - Les antennes omnidirectionnelles (gain variant de 1 à 15 dBi<sup>2</sup>) qui ont un rayonnement sur 360°. Elles s'installent sur un point d'accès relié ou sur une carte réseau wifi.

<sup>2</sup> DeciBels Isotropes énergie moyenne rayonnée par l'antenne divisée par celle que rayonnerait une antenne idéale (isotropique) alimentée par la même puissance. Plus ce rapport est élevé plus l'onde est directionnelle.



- Les antennes directionnelles (gain allant de 15 à 24 dBi) dont le rayonnement est directif. Elles permettent d'établir des liaisons point-à-point mais aussi de couvrir une zone limitée (antenne sectorielle : point à multipoint). Elles sont de plusieurs types : antennes paraboles, antennes panneaux...

Les antennes utilisées sur les points d'accès peuvent être soit d'intérieur (la puissance de rayonnement est limitée, par exemple, dans la bande ISM, elle n'excède pas 100 mW) soit d'extérieur (la puissance de rayonnement est encore plus limitée, dans la bande ISM, elle n'excède pas 10 mW pour les canaux 8 à 13).

#### Antennes sectorielles



plat



demi-cylindre

#### Antennes directionnelles



Yagi : entre immeubles proches



Parabolique : immeubles éloignés



Panneau (patch)

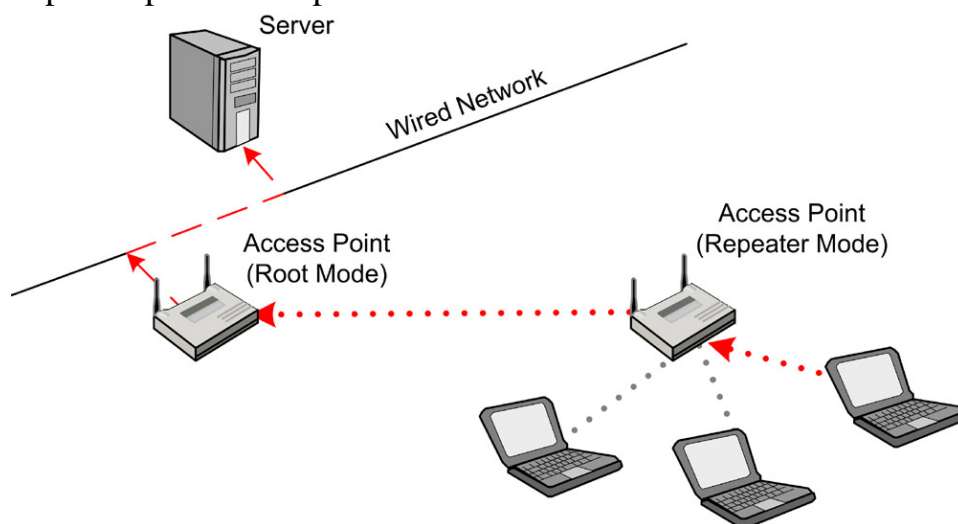
La connectique standard est de type N mais il existe d'autres connectiques utilisées par certains constructeurs : TNC-RP (Cisco, Linksys), SMA (Dlink).

- **Point d'Accès (AP) ou bornes sans fil :** en mode infrastructure, cet équipement peut être assimilé à un concentrateur, il assure la communication entre les différentes stations WiFi (les méthodes d'accès utilisées, prévues par la norme IEEE 802.11, sont décrites dans chapitres II et III). Un AP est généralement raccordé à un réseau filaire (appelé système de distribution et noté DS), par exemple Fast Ethernet, il permet de donner un accès à ce réseau.

En mode client sans fil un point d'accès fonctionne autant que client d'un autre point d'accès. Il est ainsi possible de brancher au premier point d'accès (ethernet par exemple) un périphérique ne disposant pas d'une carte wifi et accéder ainsi second point d'accès.

En mode pont, ou « wireless bridge », deux réseaux (LANs utilisant éventuellement des protocoles différents de niveau 2) peuvent être connectés par un lien sans fil en point à point. Les deux APs, de part et d'autre du lien sans fil, doivent être configurés en mode « wireless bridge ». Le mode pont peut aussi être point à multi-points pour interconnecter plus de 2 ponts d'accès.

Un autre mode appelé mode répéteur, ou « wireless repeater » ou encore « range expander », existe et permet d'étendre la portée d'un premier AP (« root mode ») par un second AP (« repeater mode »). Ce dernier ne réalise qu'une fonction de répétition. A la différence du mode pont, les protocoles de part et d'autre de l'AP répéteur doivent être identiques (l'AP n'assure aucune conversion de format de trame). L'inconvénient est que la bande passante est divisée de moitié : une première moitié est utilisée pour l'émission et l'autre moitié pour la réception (double le nombre de trames). Il est conseillé de ne pas dépasser plus de 2 répéteurs.



De la même façon que le mode pont, le mode WDS « Wireless Distribution System » assure une interconnexion sans fil d'APs. Suivant le système WDS, un AP peut jouer l'un des rôles suivants :

- « Remote Base Station » permettant de prendre en charge les clients WiFi et de passer le trafic aux APs jouant l'un des 2 rôles suivants ;
- « Main Base Station » permettant la connexion à un réseau filaire ;
- « Relay Base Station » permettant de relayer le trafic provenant des clients WiFi, de « Remote Base Stations » ou d'autres « Relay Base Stations » vers des AP « Main Base Station » ou « Relay Base Station ».

Dans WDS toutes les « Base Stations » doivent utiliser le même canal et la même méthode/clé de cryptage. La bande passante est, de la même façon que pour les répéteurs, divisée par 2. Le système WDS prévoit deux modes de connectivité :

- le mode « Bridging » où l'AP ne communique qu'avec d'autres APs et
  - Le mode « Repeating » où l'AP communique en plus avec les clients WiFi.
- WDS peut être incompatible d'un produit à un autre (non certifié par la WiFi Alliance).



Un AP peut aussi fonctionner en tant que routeur (interconnexion de niveau 3). Un routeur point d'accès peut se connecter à un autre AP et fonctionner suivant le mode « AP client », cependant il ne fonctionnera plus en tant que point d'accès, seuls les équipements connectés par un réseau filaire, à ce routeur, pourront communiquer avec lui.

Un pont d'accès peut être muni de la fonction WPS « Wifi Protected Setup » qui facilite la configuration d'un nouveau client. Plusieurs méthodes d'appairage existent. Suivant une première méthode, la plus recommandée, l'utilisateur appuie (à des instants rapprochés) à la fois sur un bouton WPS sur l'AP et un autre sur le client. Suivant une autre méthode, l'utilisateur recopie sur l'AP le code PIN du client. Il est aussi possible d'utiliser une clé USB.

Un AP peut être accompagné par des services supplémentaires : serveur DHCP, fonctions de pare-feu, authentification (IEEE 802.1x), prise en charge des VLAN (IEEE 802.q), modem ADSL.

#### IV.2.2 Couverture et débit

La zone couverte et le débit dépendent des distances entre les équipements réseaux et des obstacles entre les équipements (murs, meubles, interférences avec d'autres réseaux Wi-Fi sur des bandes adjacentes, bluetooth, fours à micro ondes, autres équipements utilisant la bande ISM, personnes ...). Notons que si dans un réseau, un seul équipement est éloigné et ne peut communiquer qu'à 1Mbits/s alors les informations de contrôle pour l'ensemble du réseau sont transmises à 1Mbits, donc l'ensemble du réseau est ralenti.

Les valeurs typiques (mais tout dépend de l'antenne : puissance, gain ...) de la vitesse en fonction de la distance à l'intérieur et à l'extérieur pour les réseaux IEEE 802.11b sont données par le tableau suivant :

Débit	Distance à l'intérieur	Distance à l'extérieur
11 Mbits/s	50 m	200 m
5,5 Mbits/s	75 m	300 m
2 Mbits/s	100 m	400 m
1 Mbits/s	150 m	500 m

Pour les normes IEEE 802.11a/g, la portée des réseaux à plus haut débit est cependant moindre. Le tableau suivant donne les valeurs typiques de la vitesse théorique en fonction de la distance à l'intérieur pour la norme IEEE 802.11g.

Débit	Distance à l'intérieur	Distance à l'extérieur
54 Mbits/s	27 m	75 m
48 Mbits/s	29 m	100 m
36 Mbits/s	30 m	120 m
24 Mbits/s	42 m	140 m
18 Mbits/s	55 m	180 m
9 Mbits/s	75 m	250 m
6 Mbits/s	90 m	400 m



### IV.3 Plan de câblage

La mise en place d'un réseau local nécessite des travaux de câblage. C'est d'ailleurs le cas pour les systèmes téléphonique, vidéo, électrique ou encore de contrôle d'accès. Le câblage comprend la pose des câbles, des boîtiers et des prises et la mise en place des sous-répartiteurs. Il faudra donc préalablement déterminer les emplacements des prises et les chemins adéquats en fonction du plan du bâtiment, des bureaux à desservir, des sources de bruits comme les lignes de courant fort (exemple de règles de câblage : distance d'au moins 30 cm si le câble réseau doit passer en parallèle avec un câble courant fort sur une distance de 20 m) ...

Deux solutions peuvent être envisagées : le post-câblage ou le pré câblage. Le post-câblage est réalisé pour des besoins bien précis et évolue à la demande suivant ces besoins. Cette solution est souvent opérée pour les bâtiments déjà construits. Par contre, le pré câblage consiste à effectuer les opérations de câblage d'une façon à desservir systématiquement tout le bâtiment, même les locaux non prévus par les besoins actuels. Les possibilités de connexion (types de prises) doivent être les mêmes dans tous les bureaux. Une autre caractéristique importante à la quelle doit répondre le pré-câblage est la reconfigurabilité, c'est à dire, la possibilité de réutiliser le câblage pour différents types de réseaux locaux et différents schémas de câblage (bâtiment intelligent). D'autre part, pour réduire les coûts d'installation, il convient d'intégrer la transmission de la voix, des données et des images dans une même opération de câblage. Les industriels recommandent d'utiliser des câbles différents pour la téléphonie et pour l'informatique car cette dernière nécessite de plus en plus une qualité supérieure permettant des débits importants (câblage non banalisé). Exemple le câblage d'IBM : câblage du réseau informatique d'établissement avec la fibre optique, câblage du réseau téléphonique avec le type 3, câblage du réseau capillaire avec la paire torsadée catégories 5 ou 6. A l'inverse, avec les réseaux RNIS le câblage est banalisé.

*On estime que le coût d'installation d'une prise pré-câblée est de 200 D à 400 D (selon le type de prise : pour téléphone, pour ordinateur ou les deux). Ce coût est multiplié de plus de 3 fois (voire même 7 fois) pour un post-câblage. Notons aussi que dans ces coûts, la main d'œuvre compte pour à peu près la moitié. Par rapport au coût total du matériel, on estime que le coût des câbles est d'environ 35 %, la connectique 15 %, l'infrastructure 45 % et 5 % d'autres frais divers.*

Le plan de câblage s'organise en deux parties : un câblage vertical ou d'établissement (BAN) et un câblage horizontal ou départemental (DAN). Ces deux types de câblage sont articulés grâce aux répartiteurs.

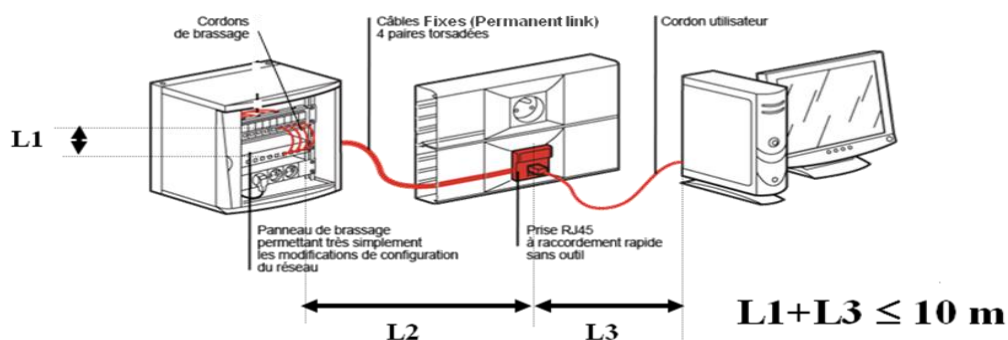
### IV.3.1 Câblage départemental

Pour le câblage départemental, la topologie physique retenue est l'étoile où l'élément central est un répartiteur situé dans un local technique (d'étage) avec les équipements actifs. Le rayon couvert par le répartiteur est de 100 m (L'ANSI recommande 295 pieds). Le nombre de prises à installer est d'une pour une surface comprise entre 6 m<sup>2</sup> et 12 m<sup>2</sup>.

Un panneau de brassage permet d'interconnecter les différents câbles provenant des équipements actifs (MAU, routeur, pont, répéteurs,...), du câblage horizontal et du câblage vertical (rocade). Le brassage permet de modifier les liaisons physiques par le simple déplacement de jarretières, d'où les possibilités de reconfiguration. Il existe aussi des panneaux de brassage électroniques (matrice de commutateurs) capable d'effectuer les opérations de brassage d'une façon programmée (figure 3).

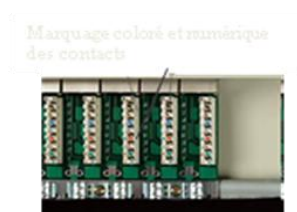
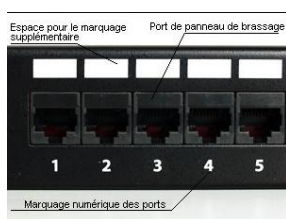
Le choix de la prise RJ45 s'est imposé. En ce qui concerne le câble c'est la paire torsadée qui est utilisée. Le câble UTP convient pour les réseaux actuels (Fast et Gigabit Ethernet). Le câble STP est aussi conseillé pour des évolutions futures (au-delà du Gigabit). Le câble SFTP est meilleur mais n'est pas nécessaire surtout lorsque le budget est limité. La catégorie 5 est la plus courante, elle est capable de supporter le Gigabit Ethernet en utilisant quatre paires (250 Mbit/s par paire). Il faut cependant que l'installation soit bien testée selon la norme TSB-95. Les nouvelles installations devraient être de catégorie 6 (supportant le gigabit).

Distance recommandées (EIA/TIA-568A /ISO 11801) :



Equipements passifs (armoires (baies,) panneaux chemins de câbles, goulottes, prises) :

#### Panneau



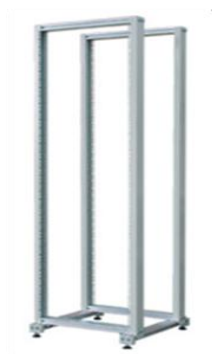
Panneau (connexion des câbles provenant des prises)



### Baies au sol ou mural



Rack (bâti, Ossature)  
à un châssis



Racks à  
double châssis



### Chemins de câbles



### Goulotte et prises



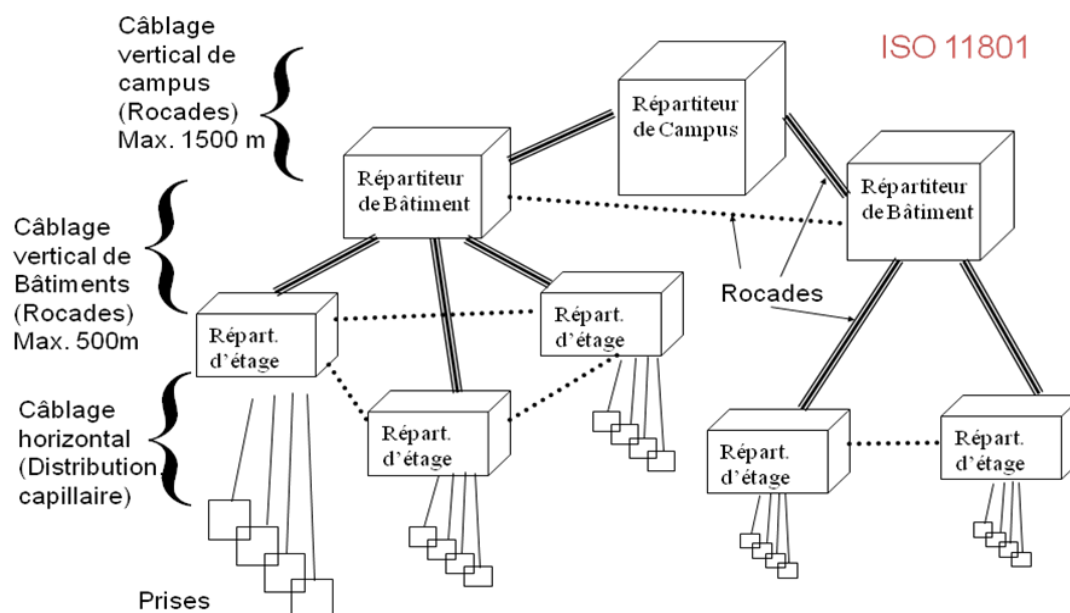
### IV.3.2 Câblage d'établissement

Une rocade relie deux locaux techniques entre eux. Elle est constituée d'un câble, ou d'un faisceau de câbles, de type paire torsadée ou fibre optique (le câble coaxial n'est plus utilisé).

Le choix de la fibre optique se justifie pour aller au-delà de 90m, il se justifie aussi lorsque on doit passer par des milieux assez perturbés (d'un bloc de bâtiment à un autre, particulièrement, dans le cadre d'un campus). La fibre optique est plus appropriée pour les évolutions futures. La fibre multimode, de plus faible coût, est la plus utilisée, cependant lorsque les distances sont importantes (à l'échelle d'un campus), la fibre monomode s'avère appropriée.

Dans une rocade, il est important de prévoir un faisceau de câbles (redondants) et ceci afin d'augmenter les possibilités de configuration, d'une façon indépendante de la disposition physique des équipements. Une rocade paires torsadées devrait comporter 25% des paires distribuées (32 paires au minimum), une rocade optique devrait comporter le double des besoins (6 fibres minimum).

Les locaux techniques d'étages sont généralement reliés à un local technique principal dit local nodal (et même à 2 locaux nodaux pour des raisons de redondance). L'interconnexion des locaux techniques par des rocades peut se faire suivant une chaîne, une boucle, une étoile ou tout autre schéma d'interconnexion. La figure suivante décrit un plan de câblage typique pour un réseau de campus.



### IV.3.3 Validation du câblage

Il existe des normes (ISO, EIA/TIA,...) concernant les performances mécaniques et électriques d'un pré câblage (prises, câbles horizontaux / verticaux, jarretière,...). Il existe aussi des normes concernant la compatibilité électromagnétique des

équipements avec leur environnement électromagnétique. La validation du câblage se fait par :

- un examen visuel : nombre, emplacement et type des prises installées ; dans les locaux techniques : ventilation, revêtement, alimentation, terre, différenciation des raccordements (ex. code couleur, étiquetage),...
- des tests statiques : grâce à un oscilloscope on peut visualiser et mesurer les temps de monter de descente d'un signal ; grâce à un réflectomètre (échomètre) on peut mesurer sur un brin les points de variation de l'impédance (ex. raccordement) et en conséquence la continuité des conducteurs,...
- des tests dynamiques : grâce à des valises de test et / ou des analyseurs de réseaux on peut effectuer des tests au niveau MAC, comme par exemple le comptage des trames, des collisions, des trames en erreurs ...

Il existe différents appareils de test et de validation :

- Echomètre : mesure de la distance du défaut en mètres ou en temps
- Certificateur de câbles (selon catégorie) : longueur, temps de propagation, atténuation, atténuation para diaphonique (Next), impédance moyenne
- Qualificateur LAN : selon la nature du réseau Ethernet 10/100/1000, qualifie la capacité d'un réseau à supporter des applications comme voix sur IP ou vidéo sur IP.



Echomètre



Certificateur de câbles



Qualificateur LAN

## V. Interconnexion des réseaux locaux

Ce chapitre est consacré à l'étude de l'interconnexion des réseaux locaux entre eux, ces derniers peuvent être sur un même site ou sur des sites distants, auquel cas, il est nécessaire de recourir à une liaison spécialisée ou un réseau intermédiaire métropolitain ou étendu.

Selon l'hétérogénéité des réseaux locaux, l'équipement d'interconnexion doit réaliser certaines opérations d'adaptations, de conversions pour faire passer une unité de données d'un réseau à un autre. Les opérations ainsi réalisées peuvent être effectuées à différents niveaux du modèle de référence OSI. La figure 1 donne une classification des équipements d'interconnexion selon les niveaux par rapport auxquels ils peuvent agir.

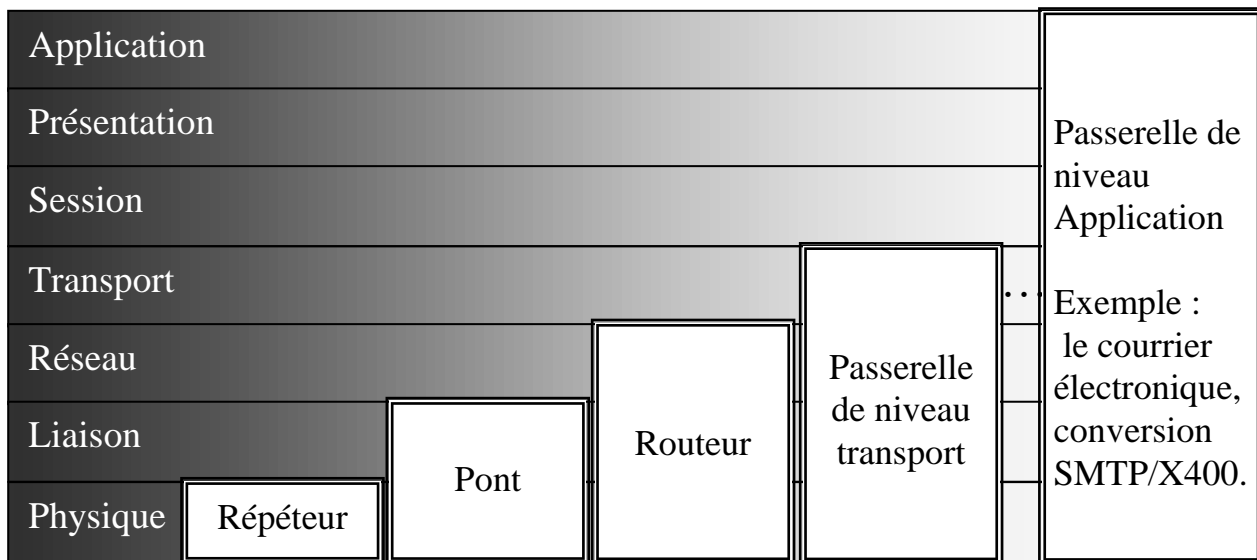


Figure 1 : classification des équipements d'interconnexion

Ce chapitre se limite à l'étude des répéteurs, des ponts et aborde l'utilisation des routeurs.

## **V.1 Les répéteurs**

### **V.1.1 Définition**

Un répéteur agit au niveau physique, il se limite à retransmettre les bits d'un médium à un autre. Le signal est ré-amplifiée (régénérée) mais aucune interprétation des données n'est effectuée.

L'utilité d'un répéteur provient du fait que la longueur du médium de transmission est en générale limitée ou aussi pour interconnecter deux supports de types différents (exemple : paire torsadée et câble coaxial).

### **V.1.2 Propriétés**

- Dans le cas d'une méthode d'accès CSMA/CD, le répéteur doit être capable de détecter et de propager une collision. De plus, le répéteur introduit un retard dont-il faut tenir compte au niveau de la tranche canal.
- Un répéteur s'utilise entre des segments ayant un même débit, il n'a donc pas besoin d'espace mémoire tampon.
- Un répéteur distant est constitué de deux demi-répéteurs reliés par un câble (exemple de la fibre optique) couvrant une certaine distance séparant les deux segments de réseau.
- Des équipements tels que les concentrateurs, HUB ou commutateurs peuvent réaliser la fonction de répétition.
- Un répéteur n'a pas besoins d'être configuré.

## **V.2 Les ponts**

### **V.2.1 Définition**

Un pont (« bridge ») agit au niveau liaison, il réalise une opération de filtrage qui consiste à examiner chaque trame pour décider s'il doit la recopier vers un réseau destination (« forwarding ») de façon à éviter la retransmission d'une trame vers un réseau où le destinataire ne figure pas.

Le recours à un pont, en subdivisant un réseau Ethernet en plusieurs sous-réseaux, permet de réduire le taux de collision. Dans le cas d'un réseau Token-Ring, une telle subdivision réduit le temps de rotation du jeton. De plus, il est possible d'effectuer plusieurs transmissions en même temps. Ainsi, le recours aux ponts permet un meilleur contrôle du trafic. Par ailleurs, la décomposition d'un réseau en plusieurs sous-réseaux, limite les effets d'une panne à un sous-réseau uniquement et protège les



sous-réseaux entre eux contre les écoutes malveillantes. Un pont est aussi utile pour remédier aux limites, de point de vue taille du réseau, imposées par certains réseaux.

### **V.2.2 Propriétés**

- La transmission à travers l'un des ports (interface LAN) d'un pont s'effectue suivant la méthode d'accès au support de transmission (auquel est connecté le port).
- La retransmission d'une trame n'est pas immédiate. Le pont doit analyser l'entête de la trame et, selon la méthode d'accès, attendre un certain délai pour pouvoir accéder au support de transmission. Il est donc nécessaire que le pont dispose d'une mémoire tampon. Des problèmes de congestion risquent de se manifester. Lorsque la mémoire tampon est épuisée, une solution consiste à ce que le pont envoie des demandes de « pause » pour une certaine durée (IEEE 802.3x).
- Un pont n'a pas besoin d'une adresse MAC, néanmoins on peut lui associer une adresse MAC (par interface LAN) utile pour la fonction de filtrage (cf. §VI.2.3). Un pont peut aussi disposer d'une adresse réseau utile pour des fonctions d'administration du pont.
- Un pont peut interconnecter deux ou plusieurs sous-réseaux.
- Un pont distant est constitué de deux demi-ponts reliés par une liaison couvrant une certaine distance séparant les deux sous-réseaux. Par exemple, la liaison peut être une liaison HDLC (respectivement un circuit virtuel X.25), une trame MAC est alors encapsulée dans une trame HDLC (respectivement, un paquet X.25).
- Lorsque les protocoles au niveau MAC sont différents, des opérations de translation et d'adaptation doivent être réalisées, cf. §V.2.4 (« Translating Bridge »).
- Lorsqu'un pont est capable de fonctionner sans que les stations, connectées aux réseaux reliés par le pont, ne se rendent compte de la présence du pont, le pont est dit transparent (« Transparent Bridge »). Un pont transparent connecte généralement des réseaux utilisant les mêmes protocoles MAC.

### **V.2.3 Algorithmes de filtrage**

Lorsqu'une trame passe par l'une des interfaces d'un pont, ce dernier doit décider s'il faut retransmettre cette trame à travers une autre interface ou non. Une première solution serait d'utiliser des tables de routage fixe chargées initialement. Cette solution est simple à mettre en œuvre mais présente un inconvénient majeur, celui de nécessiter une phase de configuration préalable du pont.

Dans la suite de cette section nous étudions différents algorithmes dit de filtrage (ou « forwarding » ou encore de pontage).



### *Filtrage transparent par apprentissage des adresses*

Le pont reste à l'écoute sur ses différentes interfaces (« promiscuous mode »). A chaque interface du pont est associée une table qui maintient l'ensemble des adresses MAC sources des trames observées sur cette interface. Ces tables, initialement vides, sont mises à jour dynamiquement à la mise en marche du pont. Une trame est redirigée à travers une interface (autre que celle d'où provient la trame) si la table associée à cette interface comporte l'adresse MAC destination de la trame. Si aucune table ne comporte cette adresse, la trame est diffusée sur les différentes interfaces (sauf sur l'interface d'où provient la trame).

La durée de vie des entrées dans une table doit être limitée car une station peut être éteinte ou même déplacée vers un nouveau sous-réseau. A cet effet, à chaque entrée d'une table est associé un délai de garde. Une entrée de la table disparaît si la station, ayant l'adresse MAC maintenue par cette entrée, ne transmet aucune trame durant le délai de garde. Le temporisateur (par défaut, 20 sec.) associé à une adresse MAC est systématiquement réarmé à chaque fois qu'une trame, issue de cette adresse, est observée (cette adresse peut changer d'une table à une autre). Le pont est ainsi capable de mettre à jour ces tables par auto-apprentissage, il est donc transparent.

L'algorithme décrit n'est pas valable si le réseau comporte une boucle de ponts (cf. figure 2). Supposons qu'une trame est émise par la station 1 vers la station 2, les deux ponts A et B mettent à jour leurs tables puis retransmettent la trame. La station 2 va recevoir deux copies de la trame, bien plus, les ponts A et B vont supposer que la station 1 est raccordée au segment Y. Les algorithmes décrits dans ce qui suit traitent le problème des boucles.

Remarque : Le recours à des boucles est nécessaire lorsqu'on veut réaliser des chemins alternatifs afin de distribuer la charge de communication ou aussi pour une meilleure tolérance aux pannes.

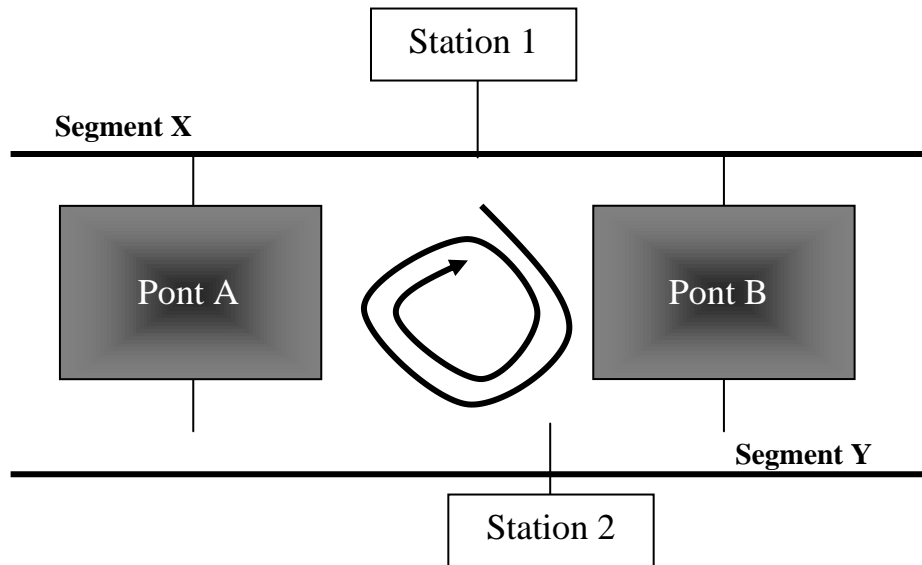


Figure 2 : exemple de réseau comportant une boucle

#### *Algorithme de l'arbre recouvrant « spanning tree »*

##### Principe :

Une solution au problème posé par les boucles est de déterminer un arbre recouvrant le réseau. Les nœuds de l'arbre représentent les ponts et les arêtes représentent les sous-réseaux. Les ponts ne peuvent ainsi router qu'à travers les arêtes de l'arbre.

Cet Algorithme, décrit dans la spécification IEEE 802.1D, a été retenu pour l'interconnexion des réseaux IEEE 802.3.

##### Construction de l'arbre :

- L'algorithme est distribué, il s'exécute sur les différents ponts du réseau.
- A chaque pont est attribué un identificateur (niveau de priorité (2 oct.) adresse + adresse MAC) unique dans le réseau. Le pont, ayant la plus petite identification, est élu racine de l'arbre. Initialement chaque pont se considère comme étant la racine de l'arbre.
- Chaque port (interface) d'un pont sera identifié par un numéro (niveau de priorité (2 oct.) adresse + adresse MAC).
- Le coût d'une route est comptabilisé en nombre de sauts et/ou dépendant du débit des ports (inversement proportionnelle au débit de l'interface d'un port =  $1000 / \text{débit (en Mbits/s)}$ )
- Au niveau de chaque pont et lors de la détermination d'une route vers la racine, le choix de la route se fait en retenant le plus court chemin. S'il existe plusieurs

routes de même coût, la route choisie est celle qui passe par le pont de plus faible identité. Si en plus plusieurs meilleures routes passent par un même pont, la route choisie est celle qui passe par le port de plus faible numéro.

- Les ponts échangent entre eux des messages de configuration traduisant des propositions de routes vers une racine supposée (pouvant différer d'un pont à un autre). Ces messages comportent les informations suivantes :

- l'identité supposée de la racine,
- le coût de la route vers la racine,
- l'identité du pont ayant émis le message,
- le numéro du port à travers lequel le message est émis.

- Chaque pont maintient la meilleure configuration trouvée (CONFIG). Celle-ci est décrite comme suit :

CONFIG = [ identité supposée de la racine,  
coût de la route vers cette racine,  
identité du pont local,  
numéro du port vers la racine ]

- A chaque port est associée un meilleur message de configuration observé sur ce port. Soient  $C=(c1,c2,c3,c4)$  et  $D=(d1,d2,d3,d4)$  deux messages de configuration, le message C est meilleur que D si :

$[c1 < d1]$  ou  $[(c1 = d1) \text{ et } (c2 < d2)]$  ou  $[(c1 = d1) \text{ et } (c2 = d2) \text{ et } (c3 < d3)]$  ou  $[(c1 = d1) \text{ et } (c2 = d2) \text{ et } (c3 = d3) \text{ et } (c4 < d4)]$ .

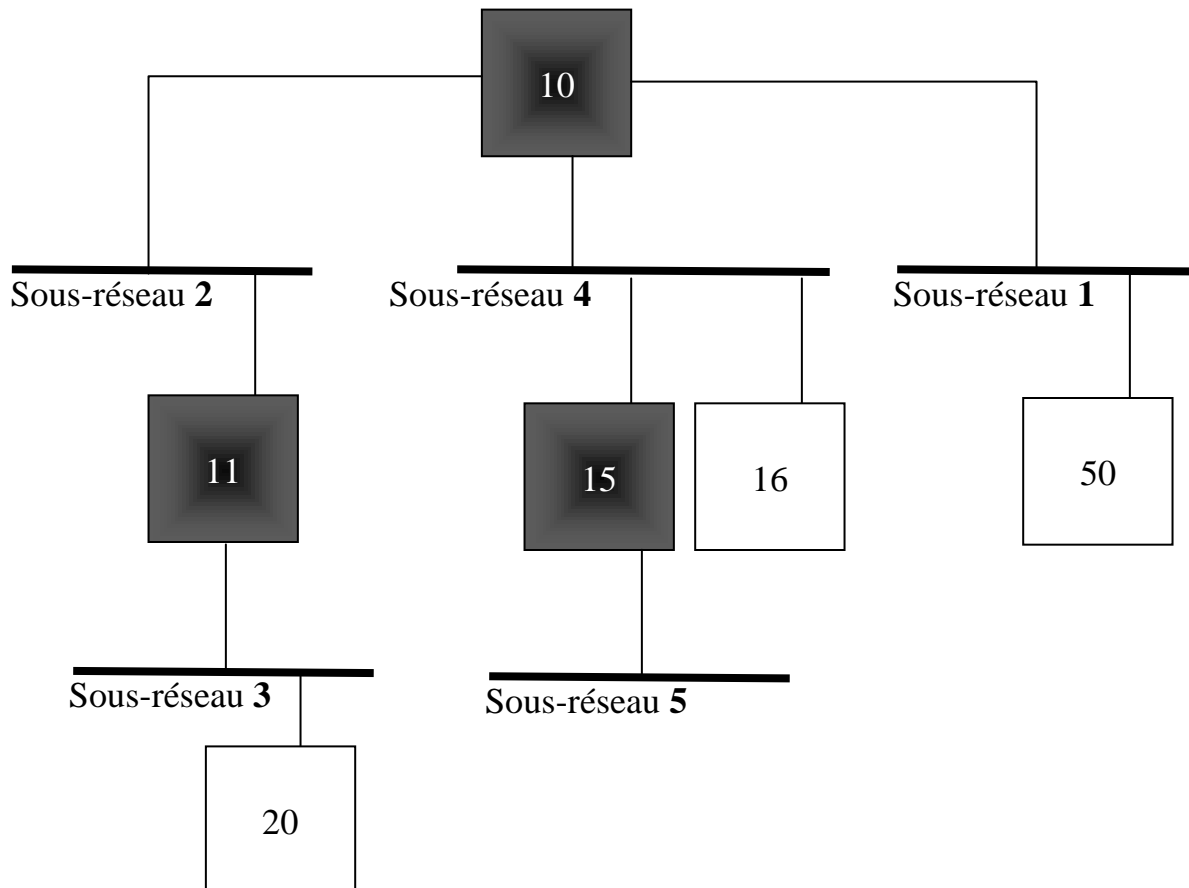
- Un port, mis à part celui menant vers la racine, ayant une meilleure configuration (et si celle-ci correspond à un message envoyé par un pont voisin et non le pont local) que CONFIG est désactivé (une fois que le meilleur message associé au port a été déjà pris en compte dans le calcul de CONFIG). La désactivation a lieu une fois que les ponts arrivent à un état stable, elle est en conséquence retardée 15 secondes.
- Périodiquement et à chaque modification de CONFIG, un message de configuration est envoyé à travers les différents ports. Le pont est ainsi capable de tenir compte des modifications (de la topologie, des priorités ...) affectant le réseau.

Exemple : voir la figure 3 et 4.

Critiques :

- Facilité d'installation grâce au fonctionnement transparent des ponts. Les stations n'interviennent pas dans l'exécution de l'algorithme de routage.

- Sous utilisation du réseau : les routes alternatives ne sont pas utilisées (cf. figure 4).
- Les ponts les plus proches de la racine risquent d'être des goulots d'étranglement.
- Tel qu'il est décrit, l'algorithme est mal adapté pour les réseaux de grandes tailles, le temps de calcul de l'arbre devient important. Un partitionnement du réseau est alors nécessaire.



*Figure 3 : arbre résultant*

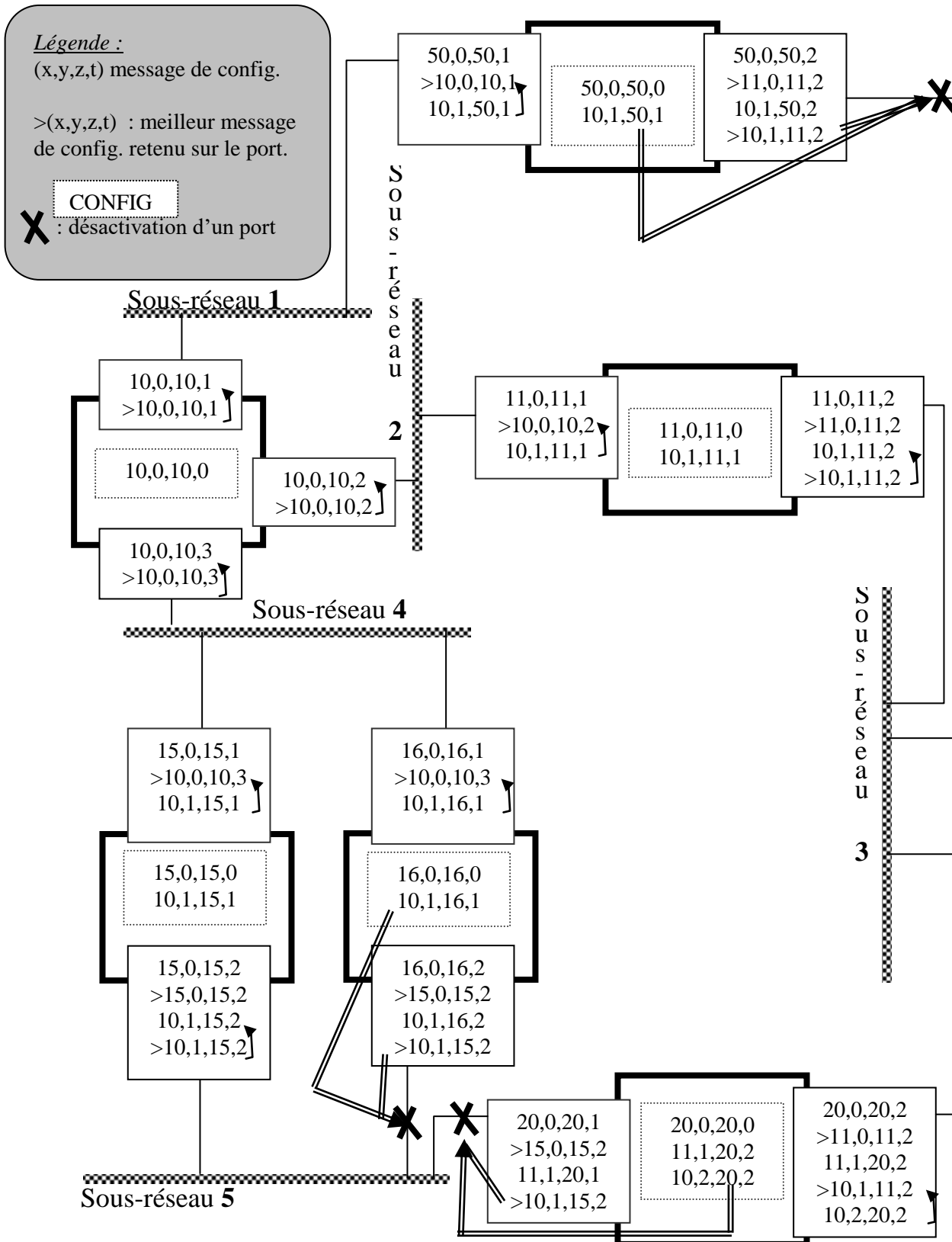


Figure 4 : exemple de déroulement de l'algorithme « spanning tree »

### **Algorithme de routage par la source « source routing »**

Suivant cet algorithme de routage, le choix de la route vers une destination est laissé à la charge de la source. Celle-ci envoie une trame d'exploration en diffusion afin d'explorer toutes les routes « All Path Explorer ». A chaque passage par un pont, celui-ci rajoute son identification ainsi que l'identification du sous-réseau source (en conservant l'ordre de passage par les différents ponts déjà traversés). Par la suite, le pont retransmet la trame sur tous ses ports sauf d'où est parvenue la trame. Si une trame d'exploration revient à un pont, elle est éliminée. Le destinataire répond à chacune de ces trames d'exploration par une autre trame qui suit la même route que la trame d'exploration mais en sens inverse. La source choisit une route. Elle insère dans une trame de donnée la route retenue.

#### Format d'une trame (LLC/source routing/IEEE 802.5)

SD
AC
FC
Adresse destination
Adresse source
<b>Information de routage</b> <ul style="list-style-type: none"><li>- 3 bits: type=(data, All Path Explorer, Null<sup>1</sup>...)</li><li>- 5 bits: long. de la route en nombre d'éléments à traverser</li><li>- 1 bit sens d'interprétation (du premier élément ou inversement)</li><li>- 3 bits taille maximale d'une trame</li><li>- suite d'éléments : (élément1, élément2, élément3, ...)</li></ul> où élément est décrit par le couple (12 bits :numéro du sous-réseau, 4 bits: numéro du pont (relatif au LAN))
Champ information
FCS
ED
FS

---

<sup>1</sup> Non pris en compte par les ponts.

Le choix d'une route peut s'effectuer suivant différents critères, par exemple : la route indiquée par la première trame en réponse, la route la plus courte, alternance des routes. Les routes sont recalculées périodiquement.

Exemple : voir la figure 5.

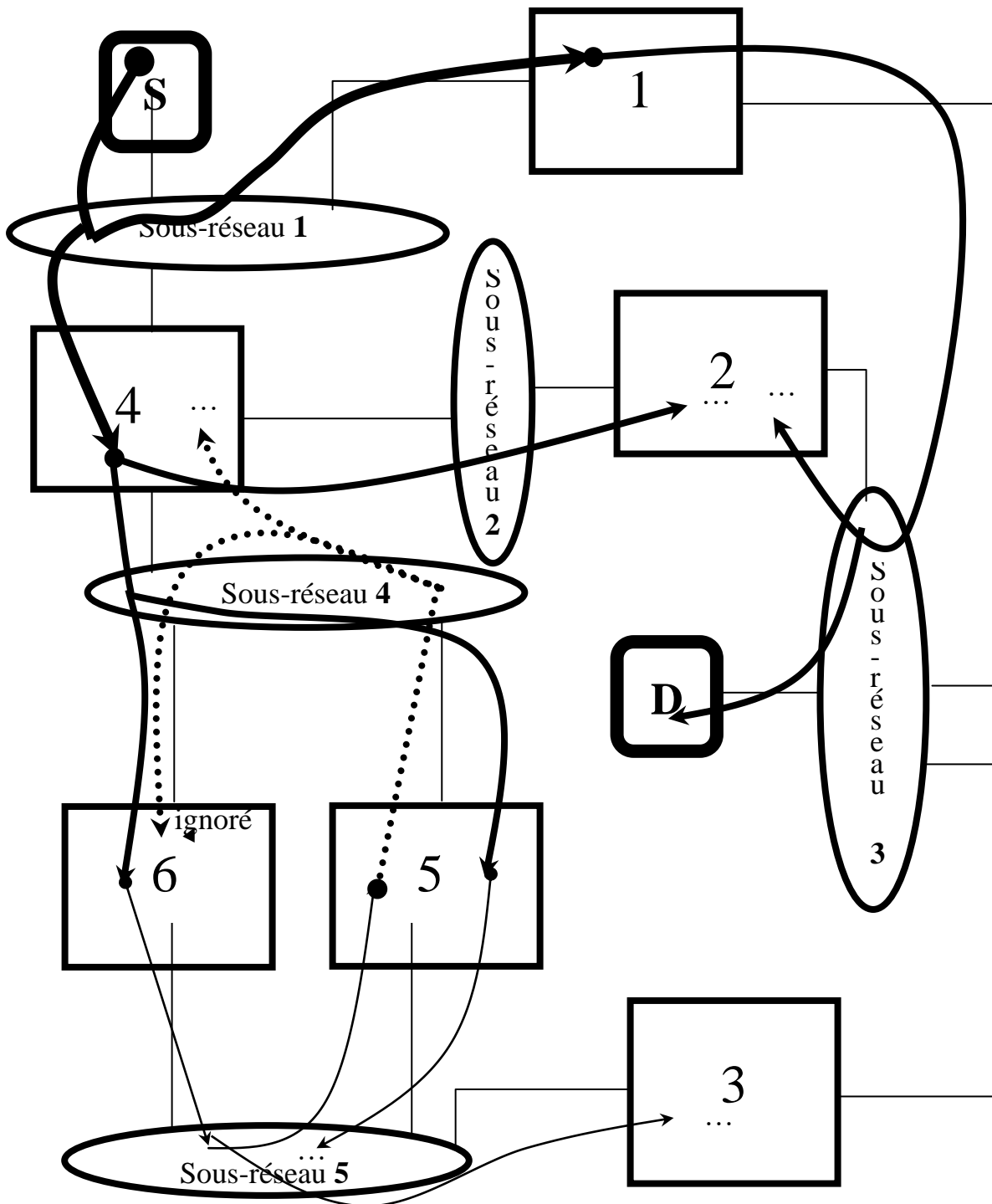


Figure 5 : exemple de routes suivies par une trame d'exploration

### Critiques :

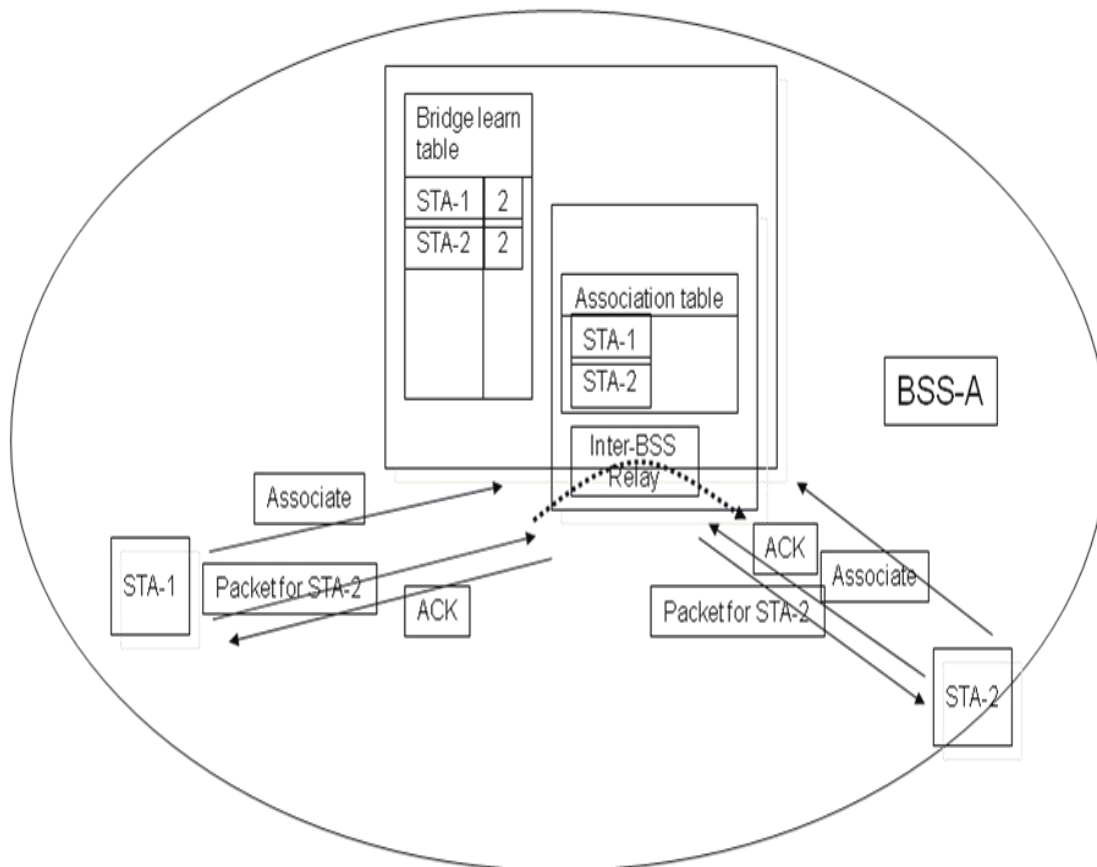
- L'algorithme optimise les routes dynamiquement et a la possibilité d'exploiter plusieurs chemins alternatifs.
- L'algorithme est non transparent, les stations doivent participer à l'exécution de l'algorithme de routage. Le traitement des pannes est aussi pris en charge par les stations.
- Un en-tête supplémentaire se rajoute au niveau de chaque trame.

### **V.2.4 Relayage des trames à travers les points d'accès**

Lors de l'association, un AP maintient la table des associations ainsi que la table des correspondances adresses MAC port (1=Ethernet, 2=PC card/Slot-A, 3=PC card/Slot-B, 4-15=WDS ports)

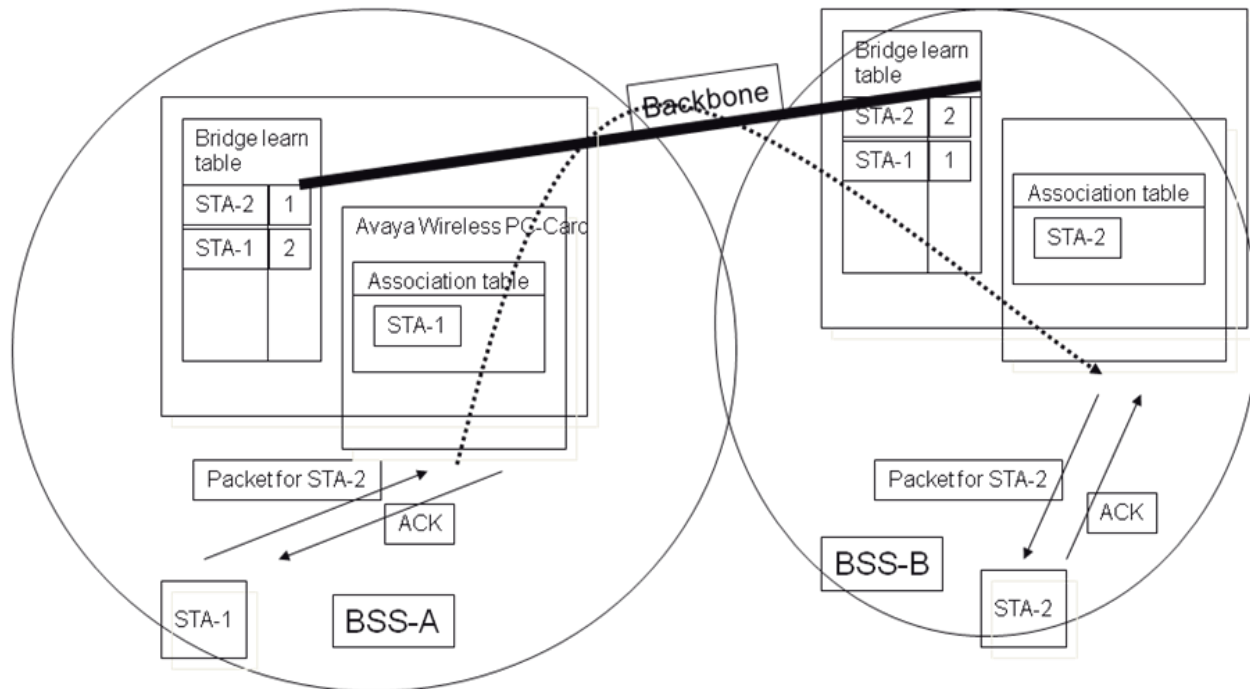
Bridge learn table	
MAC addr.	Port #.

#### ***Cas d'un BSS***

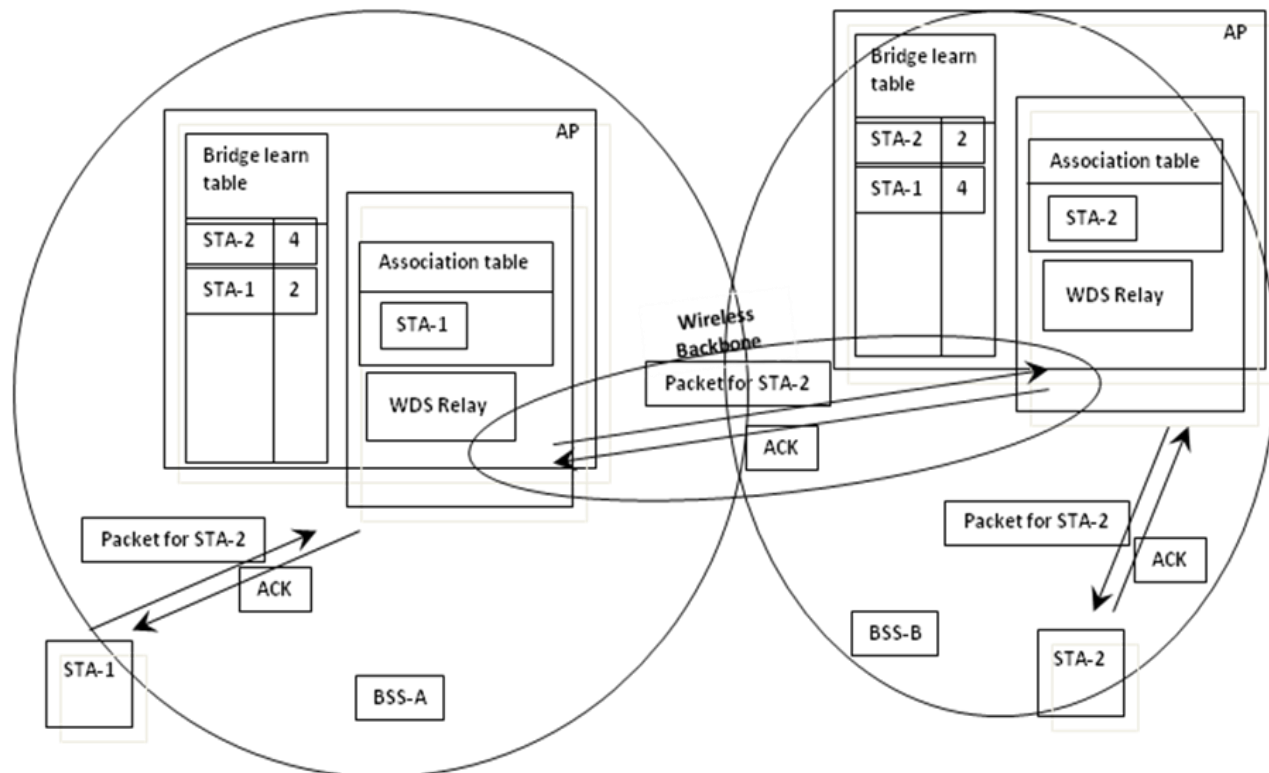




### Cas d'un ESS



### Cas d'un WDS



### V.2.5 Translation de trames

Outre les fonctions de filtrage et de relaiage (pontage), un pont doit réaliser des opérations d'adaptation, dites de translation, de trames et ceci lorsque les protocoles de niveau MAC sont différents (entre les réseaux connectés par le pont). Parmi ces opérations de translation nous avons le reformatage des trames. La taille maximale d'une trame doit être la même pour les différents réseaux interconnectés par un pont (au risque de ne pas pouvoir envoyer des trames trop longues). La solution est alors de fixer, sur chaque station, la taille maximum d'une unité de transfert (MTU) au minimum des tailles maximums supportées par différents réseaux interconnectés.

Par ailleurs, quelque soit la taille de la mémoire tampon, un pont risque de se congestionner lorsqu'il interconnecte des réseaux ayant des débits différents. Le recours à la norme IEEE 802.3x permet de retarder l'envoi de trames venant d'un pont ou d'une station en amont et ainsi résoudre le problème de surcharge.

Dans la suite de cette section, nous allons prendre comme exemple le cas d'un point d'accès (AP) qui relie un réseau Wifi à un réseau Ethernet. L'AP est considéré comme un pont, il doit effectuer un « mapping » entre :

- les champs d'une trame Wifi+entête LLC du côté Wifi, d'une part, et
- les champs d'une trame Ethernet uniquement s'il s'agit d'une trame de type 2 (DIX) ou les champs d'une trame Ethernet+entête LLC s'il s'agit d'une trame IEEE 802.3, d'autre part.

Notons que ce « mapping » est plus simple lorsqu'il s'agit d'une trame Wifi avec une trame IEEE 802.3 (puisque nous retrouvons dans ces deux trames l'entête LLC encapsulé).

Une trame Ethernet 2 est la même que celle décrite par IEEE 802.3 sauf que le champ longueur (2 octets) est remplacé par un champ type qui sert à l'aiguillage vers le protocole destination du niveau supérieur (exemple, IP : 0x0800, X.25 : 0x0805, ARP : 0x0806). Les valeurs de ce champ sont supérieures à 1500 et donc les trames Ethernet et IEEE 802.3 peuvent coexister sur le même support. La couche LLC n'existe pas. C'est la couche de niveau supérieur qui élimine les bits de bourrage.

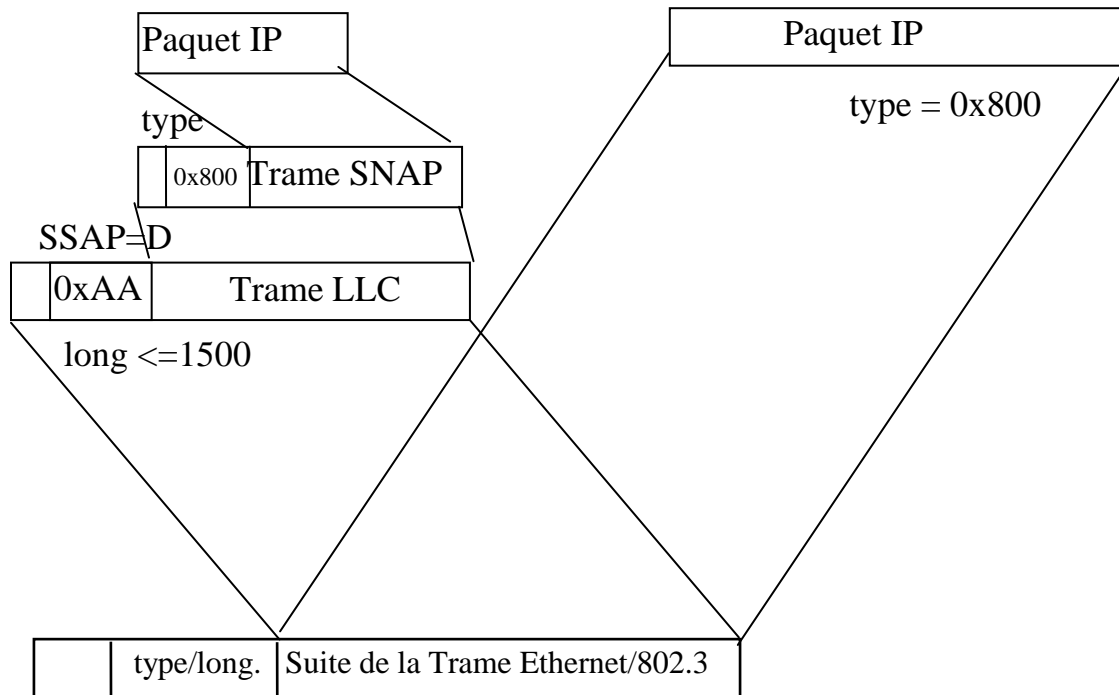


Figure 6 : différents cas d'encapsulation

Etant donné que les réseaux Ethernet 2 sont venus avant les réseaux IEEE 802.3 et qu'ainsi les logiciels de niveau supérieur (notamment ceux associés à TCP/IP) ont été développés pour les réseaux Ethernet 2, il a fallu pour les réseaux IEEE 802.3 utiliser un protocole supplémentaire SNAP « Sub-Network Access Protocol », entre la couche LLC et la couche réseau introduisant ainsi une nouvelle encapsulation (figure 6). Un entête SNAP est composé de :

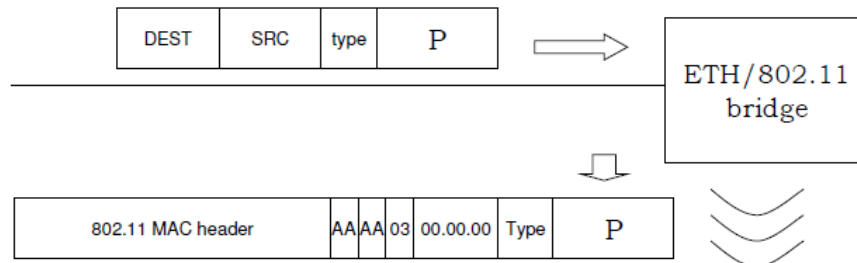
- 3 octets pour coder l'OUI (IEEE Organizationally Unique Identifier)
- 2 octets : identification d'un protocole

Suivant la RFC 1042, lorsque les 3 octets codant le OUI sont à zéro (00 00 00), les deux octets qui suivent codent le champ « type » de la trame Ethernet 2. Il est ainsi possible pour un pont d'effectuer une conversion entre une trame Ethernet 2 et une trame encapsulant LLC sans perdre la valeur du champ « type ». Cependant, un problème se pose, il vient du fait qu'Apple et Novell ont utilisé pour leur protocoles (AARP : « AppleTalk Phase 2 Address Resolution Protocol » et IPX : « Internetwork Packet eXchange ») les entêtes SNAP de la RFC1042. La norme IEEE 802.1H traite ce problème comme le décrit les paragraphes qui suivent.

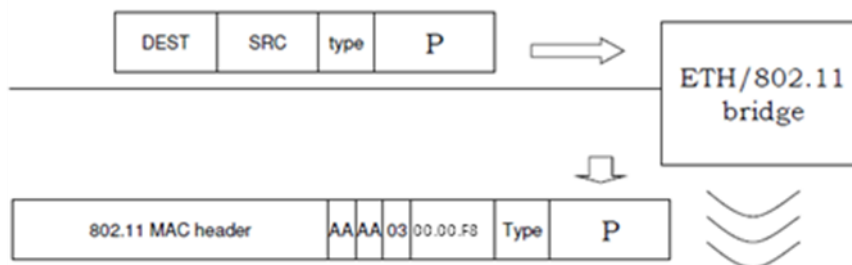
Lorsqu'une trame vient d'un réseau Ethernet et doit passer à un réseau Wifi trois cas se posent :

- si le format de la trame est celui de l'Ethernet 802.3 les entêtes LLC/SNAP restent intacts.

- si le format de la trame est celui de l'Ethernet 2 et le champ type est différents de 0x80F3 (ARP) et de 0x8137 (IPX), le point d'accès convertit la trame en une trame IEEE 802.11 et rajoute les entêtes LLC/SNAP conformément à la RFC 1042 :



- si le format de la trame est celui de l'Ethernet 2 et le champ type est égal à 0x80F3 (ARP) ou à 0x8137 (IPX), le point d'accès convertit la trame en une trame IEEE 802.11 et rajoute les entêtes LLC/SNAP conformément au protocole (BTEP) « Bridge Tunnel Encapsulation Protocol » :



#### Remarques :

- chaque pont maintient une table appelée STT : « Selective Translation Table » contenant la liste des protocoles qui doivent être traduite d'une manière sélective. Cette table contient des entrées relatives aux protocoles ARP et IPX ou uniquement le protocole ARP (car il est généralement possible de reconfigurer les stations utilisant IPX pour éviter qu'ils ne posent des problèmes lors de la suppression de l'entête SNAP/RFC 1042).
- Une station connectée au réseau Wifi doit disposer d'un pilote capable de traiter les différents empilements de protocoles possibles. Ce pilote offre une interface semblable à celle de l'Ethernet.

Lorsqu'une trame vient d'un réseau Wifi vers un réseau Ethernet, l'un des cas suivants s'applique :

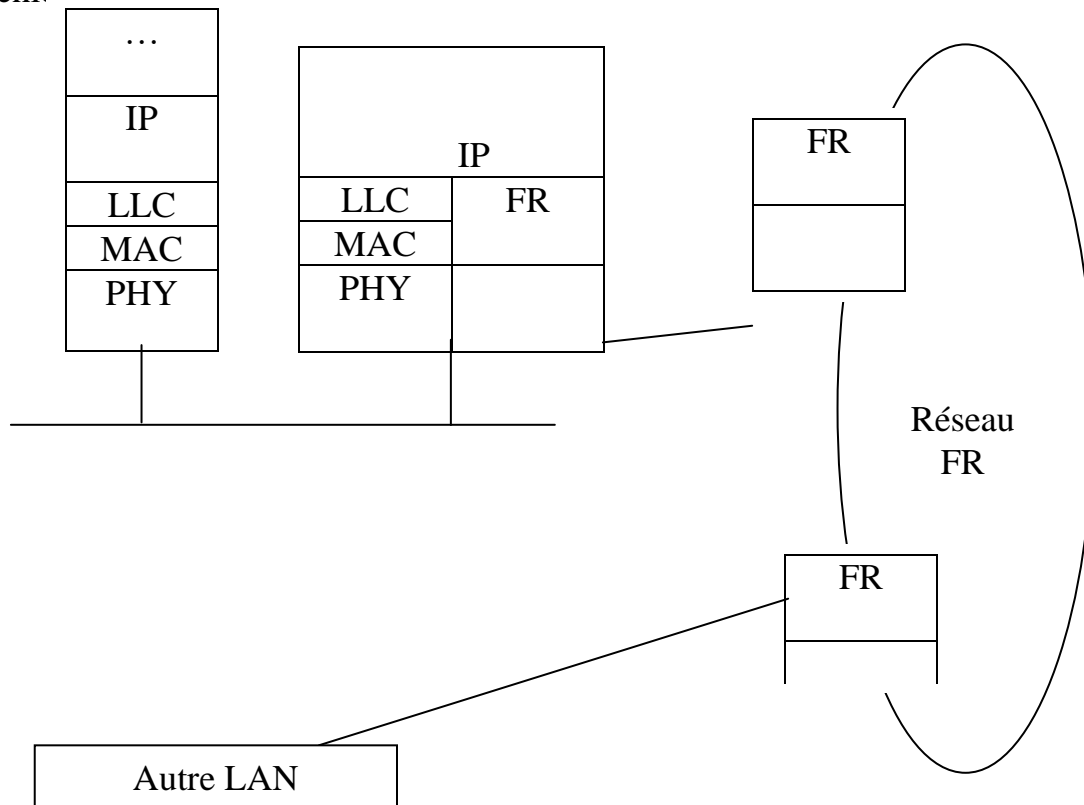
- si la trame dispose d'un entête SNAP/BTEP (commençant par 0xAA-AA-03-00-00-F8), elle est décapsulée en une trame Ethernet type 2 dont le champ type est repris à partir des 2 derniers octets de l'entête SNAP.
- si la trame dispose d'un entête SNAP/RFC 1042 (commençant par 0xAA-AA-03-00-00-00) et si les 2 derniers octets de l'entête SNAP ne sont pas dans la table STT, la trame est décapsulée en une trame Ethernet type 2 dont le champ type est repris de l'entête SNAP.

- si la trame dispose d'un entête SNAP/RFC 1042 (commençant par 0xAA-AA-03-00-00-00) et si les 2 derniers octets de l'entête SNAP sont dans la table STT, la trame n'est pas décapsulée elle reste conforme au format IEEE 802.3 et les entêtes LLC/SNAP restent intacts.
- Tout autre entête passe intacte dans le réseau Ethernet.

### V.3 Les routeurs

Un routeur agit au niveau réseau, il permet d'acheminer des paquets en fonction de l'adresse réseau du destinataire.

La figure 6 décrit un exemple d'interconnexion d'un réseau local à un réseau FR « Frame Relay ». Toutes les machines hôtes utilisent le protocole IP au niveau de la couche réseau. Les trames FR sont utilisés pour encapsuler les paquets IP et ainsi les véhiculer.



*Figure 7 : interconnexion D'un LAN à travers un réseau FR*

Il est aussi utile d'interconnecter différents sous-réseaux locaux entre eux à travers un routeur. Comparé au recours à un pont, il est ainsi possible de s'abstraire des opérations d'adaptation à effectuer au niveau MAC entre des réseaux de types différents.

## V.4 Les pont\_routeurs

Un pont\_routeur (« Bridge\_router » ou « B\_router ») agit au niveau de la couche réseau tant qu'il reconnaît les protocoles de ce niveau, il se comporte comme un pont dans le cas contraire.

Principales caractéristiques :

- Un routeur dispose de plusieurs ports LAN et / ou WAN. Chaque port LAN lui est associé une adresse MAC.
- Un routeur peut supporter différents protocoles de routage (RIP, EGP, OSPF...), le protocole étant fixé au moment de la configuration. De même, un pont\_routeur peut supporter différents protocoles de filtrage (« Source Routing », « Spanning Tree »).
- Il existe des routeurs multi-protocoles prenant en charge différents protocoles : IP (DoD), IPX (Novell), X25 (ISO), XNS (Xerox), ...
- Un routeur a besoin d'une mémoire tampon pour le stockage temporaire des messages en transit.
- Certains routeurs permettent de gérer des priorités entre les différents protocoles de niveau réseau.
- Un routeur est configuré grâce à un terminal qui lui est relié directement, ou aussi, à travers le réseau via un terminal virtuel.

## V.5 Exercices

### Exercice 1

Dérouler l'algorithme du « spanning tree » sur l'exemple de la figure 3 en remplaçant le pont numéroté 50 par un pont numéroté 14 et le pont numéroté 11 par un pont numéroté 21. Décrire l'arbre résultant.

### Exercice 2

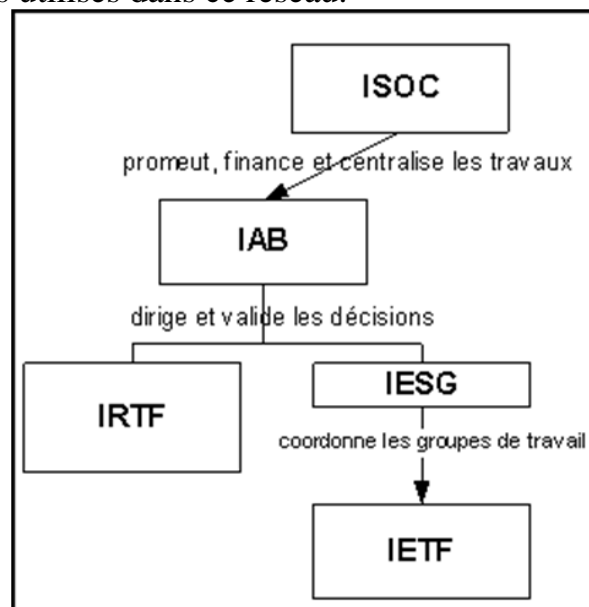
Suivant l'algorithme du « source routing », donner toutes les routes passant par le pont 6 de la figure 5.

### Exercice 3

Donner l'architecture d'un demi-pont reliant deux sous réseaux IEEE 802.3 à travers une liaison HDLC.

## VI. Les réseaux sous TCP/IP

Les protocoles TCP/IP sont issus de travaux lancés par le département de défense américain (DoD : "Department of Defense"/ DARPA : "Defense Advanced Research Projects Agency") en 1972. L'objectif étant de faire interconnecter une variété de réseaux existants. TCP/IP est officiellement retenu par le DoD en 1978 et généralisé dans ARPANET en 1983. En août 1983 l'Internet comportait 562 machines, en février 1985 ce nombre passe à 2308 et en novembre de la même année il est de 5089. L'un des premiers systèmes d'exploitation (en 1983) ayant disposé des protocoles TCP/IP est UNIX BSD qui, par son succès, a favorisé l'utilisation de ces protocoles dans les universités et dans les centres de recherche. Ceci a donné lieu au plus grand réseau informatique mondial INTERNET qui est formé d'un ensemble de sous-réseaux TCP/IP individuels. En mars 1989, Tim Berners-Lee, du CERN, propose l'idée du World Wide Web. Les années 1990 ont vu l'Internet grossir à une vitesse exponentielle sous l'impulsion du Web. En 1993, on comptait 600 sites, en 1995 plus de 15000, le WWW devient le service le plus important sur Internet. Internet est ainsi devenu un réseau ouvert aux entreprises et au grand public. Il connaît un succès énorme, d'où l'importance de poursuivre les travaux de normalisation et d'amélioration des protocoles utilisés dans ce réseau.



Issu de l'ICCB (*Internet Configuration Control Board*) fondé en 1979, le comité IAB ("Internet Activities Board"), succède en septembre 1984 à l'ICCB. En 1989, l'IAB crée deux structures : l'IETF (*Internet Engineering Task Force*) et l'IRTF (*Internet Research Task Force*). L'IAB se charge, en particulier, de l'étude des choix stratégiques pour le développement du réseau Internet et de la définition de

l'architecture générale de ce réseau. L'IRTF fonctionne plutôt comme une structure internationale de coordination des efforts de recherche à travers le monde. L'IRTF se concentre sur des expérimentations non exploitables à court terme. Les résultats obtenus par l'IRTF servent de base pour des travaux approfondis d'ingénierie et de normalisation menés par l'IETF. Après la création de l'ISOC (*The Internet Society*) au mois de janvier 1992, l'IAB s'est placé sous cette nouvelle instance de l'Internet. Cette décision va entraîner un nouveau changement de nom, l'IAB signifiant désormais Internet Architecture Board. Les propositions d'ajout, de modification, ou de normalisation sont produites sous forme de rapports techniques appelés RFC ("Request For Comments"). Les RFC sont rédigées sur l'initiative d'experts techniques, puis sont revues par la communauté Internet.

Une RFC passe généralement un long processus de révision avant sa publication. Les publications RFC se divisent en deux grandes catégories : standard et non standard. Une RFC est caractérisée par un niveau de maturité ou "state" qui traduit la position dans le chemin de standardisation :

- Standard : "Proposed", "Draft" (test), "Standard"
- Non standards : "Experimental" (en cas d'échec d'un test), "Informational", "Historic".

Un RFC est aussi caractérisé par un rang ou "status" qui traduit l'importance du standard : "required", "recommended", "elective" (option), limited, "not recommended".

Les proportions des protocoles selon le state et le status sont décrites comme suit:

		S T A T U S				
		Req	Rec	Ele	Lim	Not
S	Std	X	XXX	XXX		
	Draft	X	X	XXX		
	Prop		X	XXX		
A	Info					
	Expr				XXX	
	Hist					XXX

Les RFC sont maintenues par le NIC "Network Information Center". L'ISO a produit une normalisation de l'IP : ISO8473. Par ailleurs une nouvelle version 6 de l'IP est



produite afin de palier à certains problèmes liés à la version 4 de l'IP : épuisement des adresses, explosion des tables de routage, absence de types de données, variabilité des délais d'acheminement. Actuellement la version 4 tient une place dominante sur le marché informatique et nous nous limitons dans ce chapitre à cette version.

## VI.1 Architecture des protocoles

Les protocoles TCP/IP s'insèrent dans une architecture en couches (figure 1).

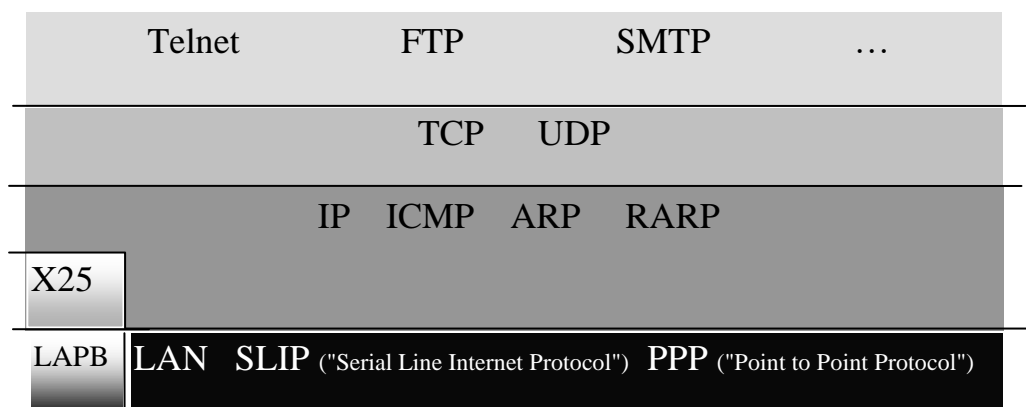


Figure 1 : Architecture TCP/IP

TCP ("Transmission Control Protocol") : protocole de transport fourni un service fiable avec connexion.

UDP ("User Datagram Protocol") : protocole de transport fourni un service non fiable sans connexion.

IP ("Internet Protocol") : protocole de niveau réseau assurant un service non fiable et sans connexion. Le transfert des paquets s'effectue en mode datagramme. A ce niveau est défini l'adressage IP. Ce protocole assure le routage, la fragmentation des unités de données ainsi qu'un contrôle de flux rudimentaire.

ICMP ("Internet Control Message Protocol") : protocoles d'échange de message de contrôle pour signaler des anomalies de fonctionnement (exemple : machine déconnectée, durée de vie d'un datagramme expiré, congestion d'une passerelle).

ARP ("Address Resolution Protocol") / RARP ("Reverse ARP") : protocoles de résolution d'adresses permettant de faire la correspondance entre les adresses logiques IP et les adresses physiques MAC. Le protocole ARP permet de déduire l'adresse MAC à partir de l'adresse IP. Le protocole RARP effectue l'opération inverse. Ceci est utile lors du démarrage d'une machine qui ne connaît pas son adresse IP mais connaît l'adresse MAC.

## VI.2 Le protocole IP (RFC 791)

Le protocole IP définit l'adressage, le format des datagrammes, la fragmentation des données et le routage.

### VI.3 Adressage (RFC990)

Une adresse IP permet de désigner de manière unique une machine. Elle est codée sur 32 bits et se divise en deux parties : le numéro du réseau (*net\_id*) suivi du numéro de la machine (*host\_id*). Un organisme international le NIC (Network Information Center) attribue les numéros de réseaux. Chaque pays a un organisme, dépendant du NIC, chargé d'attribuer les adresses IP. Le numéro de machine est attribué par l'administrateur du réseau. L'IANA « Internet Address Network Authority » est l'autorité au niveau mondial qui distribue des espaces de numéros de réseau au NIC « Network Information Center », à RIPE « Réseaux IP Européens » ... Quatre classes d'adresses sont définies, chacune code un nombre différent de réseaux et de machines:

- classe A : 1 bit = 0 ; *net\_id* = 7 bits ; *host\_id* = 24 bits.

Utilisée pour des réseaux de tailles importantes (exemple : Arpanet). Dans cette classe peuvent exister 126 réseaux, chaque réseau peut comporter plus de 16 millions de machines. Actuellement il n'est plus possible d'obtenir des adresses de cette classe.

- classe B : 2 bits = 10 ; *net\_id* = 14 bits ; *host\_id* = 16 bits.

Utilisée pour des réseaux d'industriels, de centres de recherche ou d'université. Dans cette classe peuvent exister plus de 16000 réseaux, chaque réseau peut comporter plus de 64 milles machines. Pour cette classe aussi, on a constaté que les adresses sont sous utilisées. C'est pourquoi, il est de plus en plus difficile d'obtenir une adresse de cette classe.

- classe C : 3 bits = 110 ; *net\_id* = 21 bits ; *host\_id* = 8 bits

Utilisée pour les réseaux comportant peu de machines. Dans cette classe peuvent exister plus de 2 millions de réseaux, chaque réseau peut comporter au plus 254 machines. Si un site comporte plus de 254 machines et qu'une adresse de classe B sera sous utilisée, le NIC attribue plusieurs adresses de classe C au même site (ce qui complique le routage).

- classe D : 4 bits = 1110 ; *host\_id* = 28 bits

Utilisée pour désigner une adresse de groupe ("multicast").

Une adresse Internet est référencée par une suite de 4 entiers séparés par des points :

- classe A : [1..127].[0..255].[0..255].[0..255],
- classe B : [128..191].[0..255].[0..255].[0..255],
- classe C : [192..223].[0..255].[0..255].[0..255],
- classe D : [224..239].[0..255].[0..255].[0..255].

Il est à noter que certaines adresses sont réservées pour un usage particulier :

- un paquet émis vers une adresse, dont le *net\_id* est égale à 127, revient à l'émetteur sans passer par le réseau (boucle locale ou "loopback"),
- une adresse dont le *net\_id* est égale à 0 désigne le réseau courant,

- une adresse dont tous les bits de host\_id sont à 1 est une adresse de diffusion,
- une adresse dont tous les bits de host\_id sont à 0 et les bits du net\_id non nuls est une adresse de sous-réseau,
- 0.0.0.0 Signifie "celui-ci". C'est à dire "cette machine". Elle est utilisée par exemple par une machine sans disque qui ignore son adresse au moment du boot.
- Adresses des réseaux privés réservés :

Classe	Masque	Plages d'adresses réservés	
A	255.0.0.0	10.0.0.0	- 10.255.255.255
B	255.255.0.0	172.16.0.0	- 172.31.255.255
C	255.255.255.0	192.168.0.0	- 192.168.255.255

Remarquons que, contrairement à l'adressage ISO, la longueur d'une adresse IP est fixe. D'autre part, le host\_id peut être divisé en deux parties : une adresse pour désigner un sous-réseau et une adresse de machine. Les bits de chacune de ces parties ne sont pas forcément contigus, mais la plus part des systèmes l'exigent. Pour déterminer l'adresse d'un sous-réseau on utilise un masque ("netmask") dont la taille est de 32 bits et où les bits à 1 désignent ceux du réseau et du sous-réseau. Le masque de sous-réseau doit être identique pour tous les sous-réseaux dérivés d'un même numéro de réseau. De plus les sous-réseaux doivent être physiquement séparés par des routeurs.

#### Exemples :

- Une société dispose de 4000 stations auxquelles sont attribuées 16 adresses de réseau classe C : de 192.24.16.0 à 192.24.31.0. La valeur du netmask est alors 255.255.240.0 (à 1 tous les bits qui ne changent pas entre les adresses attribués). Il suffira alors à un routeur d'effectuer un ET logique (bit à bit) entre une adresse et le netmask pour déterminer si cette adresse est celle d'une station de la société.
- L'ENSI lui attribuée l'adresse réseau 193.95.17.0, désire diviser son réseau local en 4 sous-réseaux. Une valeur du netmask est alors 255.255.255.192.

## **VI.4 Format d'un datagramme IP (RFC 791)**

Le format d'un paquet IP est décrit par la figure 2.

0	4	8	16	31
vers. =4		lg. entête	type de service	lg. totale du datagramme
identif. Commun aux fragments			drapeau	déplacement fragment
durée de vie		protocole	checksum	
adresse source				
adresse destination				
options				
bourrage				
données				

*Figure 2 : format d'un paquet IP*

- Version (4 bits) : indique le format de l'entête. Le format décrit est celui de la version 4.
- Longueur de l'entête (4 bits) : en nombre de mots de 32 bits. Des bits de bourrage sont rajoutés à l'entête pour que sa longueur soit multiple de 32.
- Type de service (8 bits) : ce champ est utile pour le routage. Il indique la qualité de service requise (RFC1349).
  - Bits 0-2 : priorité,
  - Bit 3 : s'il est à 1 les routeurs doivent minimiser le délai de transmission (ex. éviter les liaisons satellite),
  - Bit 4 : s'il est à 1 les routeurs doivent maximiser le débit,
  - Bit 5 : s'il est à 1 les routeurs doivent suivre un chemin fiable,
  - Bit 6 : s'il est à 1 les routeurs doivent minimiser les coûts,
  - Bit 7 à 0.
- Longueur totale du datagramme (16 bits) : exprimé en octets (<65535).
- Identificateur commun aux fragments (16 bits) : tous les fragments d'un même datagramme portent un même numéro.
- Drapeau (3 bits) : le premier bit est toujours à 0. Le deuxième bit indique, s'il est à 0, que le datagramme peut être fragmenté par un routeur. Le troisième bit indique s'il est à 0 que c'est le dernier fragment d'un datagramme, par défaut la valeur est 000.
- Déplacement fragment (13 bits) : indique la position du premier octet d'un fragment dans le datagramme initial avant fragmentation. Ce déplacement s'exprime en multiple de 8 octets.
- Durée de vie (8 bits) : indique le temps maximum pendant lequel le datagramme peut rester dans le réseau. A la valeur 0 le datagramme est détruit.

Chaque routeur par lequel passe un datagramme réduit la durée de vie, d'une unité ou plus, proportionnellement à la durée passée dans le routeur.

- Protocole : indique le protocole suivant dont le paquet se trouve dans la partie donnée (ip : 0, icmp : 1, tcp : 6, udp : 17, voir RFC 1340).
- checksum (16 bits) : le checksum est la somme en complément à 1 des mots de 16 bits de l'en-tête. Il est recalculé par chaque routeur puisque le champ durée de vie est modifié.
- Adresses source, destination : tel que décrit dans la section précédente.
- option (longueur variable), ce champ est utile pour :
  - gérer des problèmes de sécurité et de confidentialité,
  - fournir aux routeurs des informations de routage par exemple un chemin désigné par une suite d'adresses,
  - connaître le chemin suivi par un datagramme,
- bourrage pour que l'en-tête soit multiple de 32 bits.

## VI.5 Le routage IP

Un réseau INTERNET résulte de l'interconnexion de plusieurs réseaux par des passerelles appelées routeurs. On distingue deux niveaux de routage : le routage à l'intérieur d'un même réseau et le routage entre les passerelles de l'INTERNET (routeur). Il est à noter qu'à chaque passage par un réseau, un datagramme est encapsulé dans un paquet conformément aux protocoles du réseau.

Dans ce qui suit nous nous intéressons au routage entre passerelles IP. Différents domaines de routage (AS : "autonomous systems") peuvent exister, chacun ayant ses propres protocoles de routage interne et externe :

- le routage interne concerne les paquets relatifs à des communications à l'intérieur d'un même domaine AS (IGP : "Interior Gateway Protocol"). Un domaine peut être aussi subdivisé en sous-domaines (exemple un LAN);
- le routage externe pour les communications entre différents domaines AS.

### Le routage RIP (RFC 1058)

Le protocole de routage RIP (Routing Information Protocol) est le plus utilisé dans l'environnement TCP/IP. C'est un routage distribué basé sur l'échange d'informations entre routeurs adjacents (toutes les 30 secondes). Chaque routeur a une connaissance partielle sur l'état du réseau qui est limitée aux voisins (algorithme de type "distant vector"). RIP est un protocole IGP prévu pour être utilisé sur des réseaux de petites tailles. Une route ne doit pas dépasser 15 nœuds intermédiaires. RIP utilise le protocole UDP pour encapsuler ses données (port 520). Plusieurs améliorations du RIP ont été proposées (exemples : RIP-2, IGRP "Interior Gateway Routing Protocol").

### Le routage OSPF (RFC 1247)

Le protocole de routage OSPF (Open Shortest Path First) est plus complexe que le routage RIP mais il est adapté aux réseaux de grandes tailles. OSPF est aussi un protocole IGP. Contrairement au RIP, chaque routeur a une connaissance complète sur l'état des liens du réseau (algorithme de type "link state"). Ceci permet notamment de résoudre les problèmes de boucles. OSPF utilise le protocole IP pour encapsuler ses données (avec le protocole numéro 89).

D'autres protocoles de routages externes sont utilisés : EGP ("Exterior Gateway Protocol"), BGP ("Border Gateway Protocol") et CIDR ("Classless Internet Domain Routing"). Ce dernier a été développé en tenant compte qu'une même entreprise pouvait avoir plusieurs adresse de classe C.

### **VI.6 Le protocole ICMP (RFC 792)**

Le protocole ICMP ("Internet Control Message Protocol") permet de rendre compte de certaines anomalies de fonctionnement. Les messages ICMP sont encapsulés dans des paquets IP (type = 0, protocole = 1) et peuvent être issus de routeurs comme de stations. Un message ICMP est soit une demande d'information soit une indication d'erreur. Il comporte en particulier au niveau des deux premiers octets un champ type et un champ code. Des exemples de messages ICMP sont illustrés dans ce qui suit.

- message pour indiquer qu'**un paquet ne peut pas atteindre sa destination** (type = 3). Les raisons peuvent être diverses : un routeur ne sait pas par où émettre le paquet (code = 0), le destinataire ne peut pas être atteint bien que le réseau le reconnaisse (code = 1), le destinataire ne prend pas en compte le protocole (code = 2), la fragmentation est nécessaire alors qu'elle est interdite (code = 3), le port transport est inaccessible (code = 4), la route proposée n'est pas valable (code = 5).
- message pour indiquer que la **durée de vie d'un paquet a expiré** (type = 11). L'expiration a lieu soit durant le transit (code = 0), soit durant le réassemblage (code = 1).
- message pour indiquer à l'émetteur de **réduire sa vitesse** d'émission. Ce message peut être émis par le destinataire ou un routeur intermédiaire. Suite à cette réduction l'émetteur peut augmenter progressivement sa vitesse (type = 4, code = 0).
- message d'écho pour tester l'**accessibilité d'une station** sur le réseau (type = 8, code = 0). En réponse un autre message ICMP est envoyé (type = 0, code = 0).

## **VI.7 Le protocole ARP ("Address Resolution Protocol", RFC 826)**

Permet de retrouver une adresse MAC à partir d'une adresse IP. Pour cela, chaque machine maintient une table de correspondance entre ces adresses. Si une adresse IP ne figure pas dans cette table, une requête ARP contenant cette adresse est diffusée. Le nœud correspondant à cette adresse répond en fournissant l'adresse MAC. Une entrée de cette table est éliminée au bout d'un certain délai si aucun trafic n'est observé à partir de la station correspondante. Le protocole RARP ("Reverse ARP") permet de déduire l'adresse IP à partir de l'adresse MAC. Ce protocole est utile pour les stations sans disque qui, au moment de l'amorçage, ne connaissent pas leurs adresses IP. A cet effet une requête RARP est diffusée et est traitée par un serveur bien déterminé.

## **VI.8 Les protocoles du niveau transport**

### **VI.8.1 Les ports**

Une fois qu'un paquet arrive au nœud destinataire, il faut délivrer les données de ce paquet à une application particulière. A cet effet est utilisé un numéro de port. Le RFC 1340 donne la liste des numéros de ports attribués aux applications connues (smtp:25, ftp:21, telnet:23, ...). Ces numéros sont compris entre 0 et 1023. Les numéros supérieurs ou égale à 1024 peuvent être attribués aux applications utilisateurs.

### **VI.8.2 Le protocole UDP (RFC 768)**

Comparé à IP, UDP n'apporte pas de fonctionnalités supplémentaires à part l'utilisation des ports. Dans un paquet IP, le champ protocole est égal à 17. Le format d'un message UDP est décrit par la figure 3.

port source (2 octets)
port destination (2 octets)
longueur (2 octets)
checksum (2 octets) sur l'entête, s'il est à 0, il n'est pas utilisé
données

*Figure 3 : format d'une unité UDP*

### **VI.8.3 Le protocole TCP (RFC 793)**

Ce protocole offre une transmission duplex fiable en mode connecté. Les segments sont délivrés dans l'ordre d'émission. Un mécanisme de contrôle de flux par fenêtre est utilisé. Le contrôle de flux est opéré sur un flot d'octets :

- une numérotation par rapport aux octets est opérée ;

- un acquittement spécifie le numéro d'octet attendu, les précédents sont donc acquittés ;
- la taille de la fenêtre de réception peut varier dans le temps ;
- les acquittements sont positifs et la retransmission est déclenchée suite à l'expiration d'un temporisateur. La valeur de ce temporisateur est dynamique, elle se calcule en fonction de certaines statistiques (le temps d'aller et de retour) ;
- les messages sont découpés en segments.

Il est aussi possible d'attribuer une priorité aux messages. Dans un paquet IP, le champ protocole est égal à 6. Le format d'un segment TCP est décrit par la figure 4. La figure 5 illustre un exemple d'invocation des primitives TCP pour l'établissement d'une connexion, l'échange de données et la libération de la connexion.

port source (2 octets)	port destination (2 octets)
numéro de séquence SEQ (4 octets), initialisé à partir d'une horloge	
acquittement (4 octets), contient le numéro de séquence du prochain octet attendu	
-déplacement (4 bits), indique la taille de l'entête en mots de 32 bits	
-6 bits réservés à un usage ultérieur	
-6 bits (URG : urgent, ACK : le champ acquittement est significatif, PSH : transmission immédiate, RST : réinitialisation d'une connexion, SYN : initialisation d'une connexion, FIN : fin d'une connexion)	
-fenêtre (2 octets), nombre d'octets que le récepteur peut accepter (à partir du numéro de séquence acquitté)	
-checksum (2 octets), de l'entête	
-pointeur message urgent (2 octets), lorsque URG est à 1 ce champ indique le numéro de séquence du dernier octet d'une séquence d'octet qu'il faut délivrer au plutôt à la couche de niveau supérieur.	
option + bourrage, permet par exemple de définir la taille maximale d'un flot	
données.	

*Figure 4 : Format d'un segment TCP*



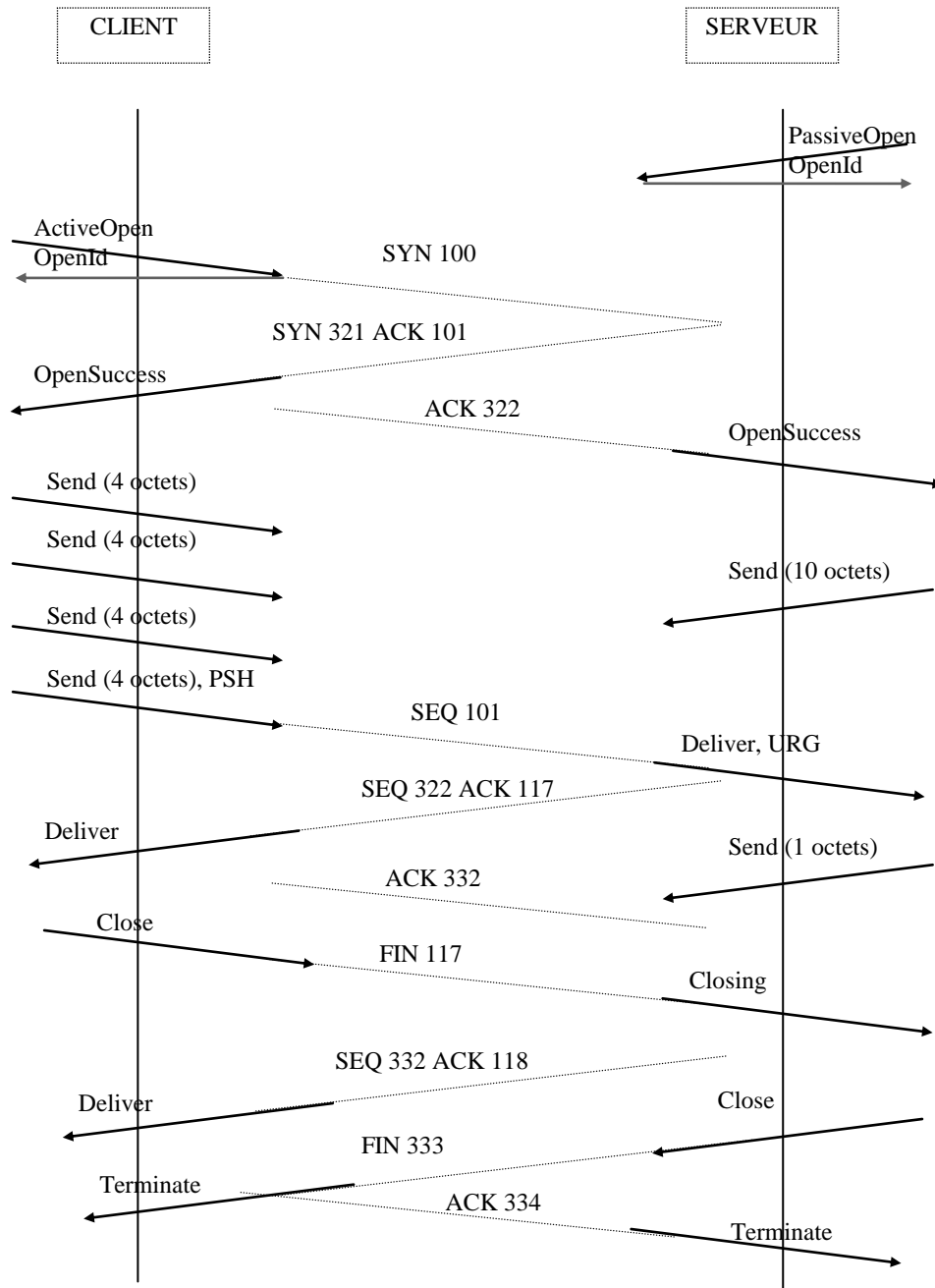


Figure 5 : exemple d'invocation de primitives TCP

## VI.9 Le service DNS

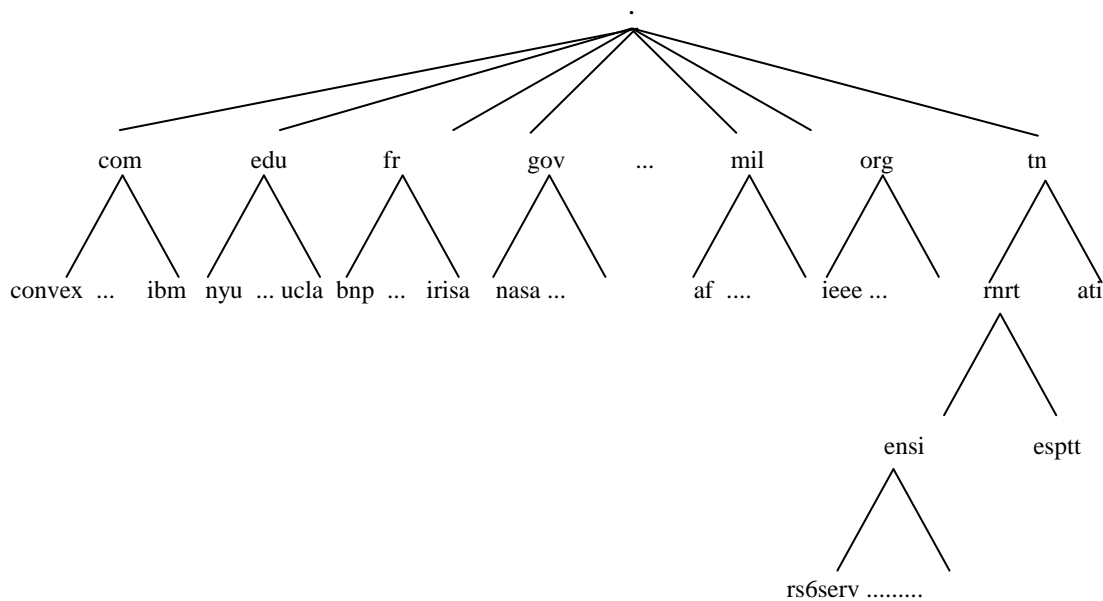
A une machine est associé un nom symbolique absolu :

*nom\_machine.domaine*

les domaines (zones) sont structurés de façon hiérarchique en plusieurs sous domaines comme le montre la figure 6. Un sous-domaine peut comporter plusieurs sous-domaines. Les feuilles de l'arbre correspondent aux noms de machines. Dans la figure 6, seule la machine rs6serv est représentée « rs6serv.ensi.rnrt.tn ».

La correspondance entre les noms et les adresses IP est maintenue par le système UNIX dans le fichier /etc/hosts. La mise à jour de ce fichier sur toutes les machines, à

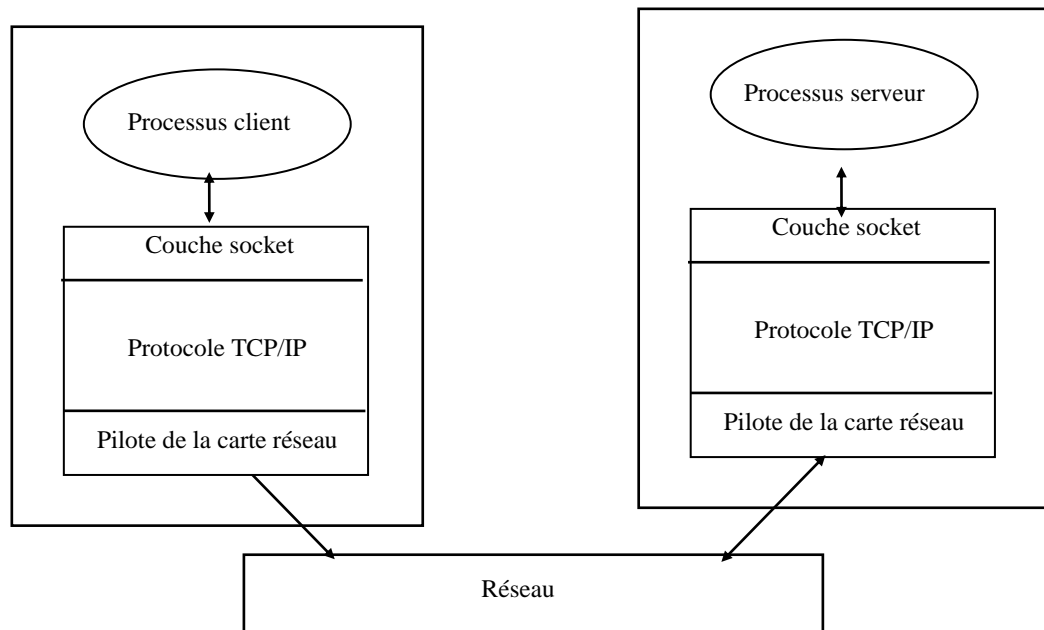
chaque fois qu'une nouvelle machine se rajoute, est impossible. Un service distribué de noms pour toutes les machines a été conçu : le DNS (« Domain Name Service »). Le DNS permet la traduction de noms en adresses et vice-versa. A cet effet le DNS utilise des serveurs de noms. Un serveur de noms gère éventuellement un ou plusieurs domaines / sous-domaines. Pour palier au problème d'indisponibilité d'un serveur de noms (primaire), des serveurs de noms secondaires peuvent être mis en place. Sans pouvoir modifier les données, un serveur secondaire est capable de traiter les demandes de résolution adressées au serveur primaire.



*Figure 6 : hiérarchie des domaines*

## **VI.10 Les sockets - programmation d'une application client/serveur**

Les sockets ont été introduites dans UNIX BSD (Berkeley, 1983) afin d'offrir un mécanisme général de communication inter-processus sur un même système ou sur des systèmes distincts. Les sockets constituent une interface pour la programmation réseau (figure 7).



*Figure 7 : le niveau sockets*

A l'intérieur d'un programme, une socket est identifiée par un descripteur permettant de spécifier un point de communication par lequel un processus peut émettre ou recevoir des informations. Le format de ce descripteur diffère selon le domaine de communication. Différents domaines sont définis :

- domaine AF\_UNIX, utile lorsque la communication se fait entre processus sur une même machine. Une socket est identifiée par une chaîne de caractères ;
- domaine AF\_INET, utile lorsque la communication se fait entre processus sur des machines reliées par un réseau internet. Une socket est identifiée par : un numéro de port et une adresse IP.
- autres domaines : AF\_NS (XEROX), AF\_CCITT (X25), AF\_SNA ...

A une socket est associé un type définissant les propriétés de communication :

- type SOCK\_DGRAM, il correspond à un service datagramme (utilisant UDP),
- type SOCK\_STREAM, il correspond à un service circuit virtuel (utilisant TCP),
- type SOCK\_RAW, un telle socket permet l'accès aux protocoles de plus bas niveau (IP, ICMP, ...), l'usage est réservé aux super-utilisateurs pour implanter de nouveaux protocoles.

Dans ce qui suit, nous décrivons les différentes primitives pour la manipulation des sockets à travers un exemple de programmes client / serveur. L'exemple est relatif à une communication en mode connecté (SOCK\_STREAM). Nous nous limiterons à des commentaires au niveau du code de ces programmes.

#### Exemple

```
/* Programme serveur : affiche les messages qui proviennent des clients */

#include <stdio.h>
#include <sys/socket.h>
#include <sys/types.h>
#include <netinet/in.h>
#include <netdb.h>

void main()
{
int sock_ecoute, sock_dial ;      /* sock_ecoute est utilisée par le processus père pour l'écoute des demandes
de
                                connexions, sock_dial est utilisée par un fils pour communiquer avec un client
                                */

char tampon[256] ;                /* pour stocker un message reçu */

struct sockaddr_in adr_serv ;     /* adresse socket serveur */
int lg_adr_serv ;                 /* longueur de l'adresse de la socket serveur */
char nom_serv[30];                /* nom du serveur */
struct hostent *num_ip_serv ;     /* pointeur sur une structure donnant le nom, l'adresse IP, etc, du serveur */
struct sockaddr_in adr_client ;  /* adresse socket distante */
int lg_adr_client ;              /* longueur de l'adresse de la socket client */

/* création de la socket d'écoute */
sock_ecoute = socket(AF_INET, SOCK_STREAM,0) ;

/* la socket est attachée à une adresse IP et un numéro de port
   (IPPORT_USERRESERVED, ne nécessite pas un mode privilégié) */
bzero((char *)&adr_serv, sizeof(adr_serv)) ;
adr_serv.sin_port = IPPORT_USERRESERVED ;
adr_serv.sin_addr.s_addr = INADDR_ANY; /*pour accepter une adresse quelconque (0.0.0.0) */
/* autre solution pour obtenir l'adresse IP de la machine locale : */
gethostname(nom_serv, (size_t) 30);
printf("nom du serveur %s \n", nom_serv);
if ((num_ip_serv=gethostbyname(nom_serv))==NULL)
{ printf(" échec dans l'obtention de l'adresse IP du serveur \n");
  exit();
}
else
{ bcopy(num_ip_serv->h_addr,&adr_serv.sin_addr,num_ip_serv->h_length);} /* fin solution */
adr_serv.sin_family = AF_INET ;
bind (sock_ecoute, (struct sockaddr*)&adr_serv, sizeof(adr_serv)) ; /* attachement de la socket */
```

```
/* ouverture du service : création d'une file d'attente pour les demandes de connexion d'une longueur max.
égale à 5*/
```

```
listen(sock_ecoute,5);
```

```
for (;;)/* boucle infinie traitant les différentes des clients */
```

```
{
```

```
/* attente d'une demande de connexion */
```

```
lg_adr_client = sizeof(adr_client);
```

```
sock_dial=accept(sock_ecoute, (struct sockaddr *)&adr_client, &lg_adr_client);
```

```
/* création d'un processus fil */
```

```
if (fork() ==0)
```

```
{ /* fils */
```

```
close(sock_ecoute);
```

```
/* réception d'un message sur la socket au moyen de la primitive read. IL existe une autre primitive de
réception « recv », celle-ci utilise un paramètre supplémentaire « in t flag » (en dernier param.) permettant de
consulter des données sans les prélever (flag=MSG_PEEK), ... */
```

```
read(sock_dial,tampon,sizeof(tampon));
```

```
printf("Le serveur a reçu : %s\n", tampon);
```

```
exit();
```

```
}
```

```
close(sock_dial);
```

```
} /* for */
```

```
}/*main*/
```

---

```
/* Programme client : envoie un message à un serveur */
```

```
#include <stdio.h>
```

```
#include <sys/socket.h>
```

```
#include <sys/types.h>
```

```
#include <netinet/in.h>
```

```
#include <netdb.h>
```

```
#include <string.h>
```

```
main(int n, char*param[])
```

```
{
```

```
int sock_vers_serv; /* sock_vers_serv utilisée pour envoyer au serveur un message */
```

```
struct hostent *num_ip_serv; /* pointeur sur une structure donnant : nom, @ IP; ... du serveur */
```

```
struct sockaddr_in adr_serv; /* adresse socket serveur*/
```

```
int lg_adr_serv; /* longueur de l'adr. la socket serveur*/
```

```
struct sockaddr_in adr_client ;    /* adresse socket distante*/
int lg_adr_client;                /* longueur de l'adresse de la socket client*/

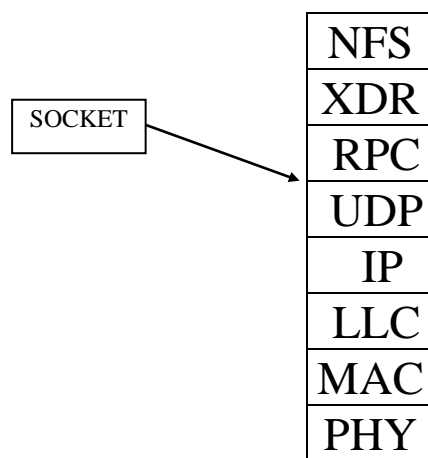
char message[256] ;

/* création de la socket vers le serveur */
if ((sock_vers_serv = socket(AF_INET, SOCK_STREAM,0))== -1)
{ printf("echec création de la socket vers le serveur\n");
  exit() ;
}
/* la socket est attachée à une adresse IP et un numéro de port
(IPPORT_USERRESERVED+1) */
bzero((char *)&adr_client, sizeof(adr_serv)) ;
adr_client.sin_port = IPPORT_USERRESERVED+1 ;
adr_client.sin_addr.s_addr = INADDR_ANY ;
adr_client.sin_family =AF_INET ;
bind (sock_vers_serv, (struct sockaddr*)&adr_client, sizeof(adr_client)) ;

/* connexion au serveur*/
bzero((char *)&adr_serv, sizeof(adr_serv)) ;
if ((num_ip_serv=gethostbyname(param[1]))==NULL)
{ printf(" nom de la machine serveur inconnu \n");
  exit() ;
}
else
{ bcopy(num_ip_serv->h_addr, &adr_serv.sin_addr,num_ip_serv->h_length) ;
}
adr_serv.sin_port = IPPORT_USERRESERVED ;
adr_serv.sin_family =AF_INET ;
if (connect (sock_vers_serv, (struct sockaddr*)&adr_serv, sizeof(adr_serv))== -1)
{
printf(" echec connexion \n") ;
exit() ;
}
strcpy(message,param[2]);
printf("%d\n", sizeof(message));
/* émission d'un message sur la socket au moyen de la primitive write. IL existe une autre primitive d'émission
« send », celle-ci utilise un paramètre supplémentaire « in t flag » (en dernier param.) permettant d'envoyer des
données de façon express (flag=MSG_OOB), ... */
write (sock_vers_serv,message ,sizeof(message) );
}
```

### VI.11 Appel de procédure à distance

L'appel de procédure à distance RPC (« Remote Procedure Call ») consiste à transférer le contrôle du programme à une procédure s'exécutant sur une machine distante. Ceci implique le passage d'arguments et le retour de résultats (comme c'est le cas pour un appel de procédure en local). Les machines appelant et appelée peuvent représenter les données différemment (entier, caractère,...), c'est pourquoi est utilisé en général un protocole pour la représentation des données de façon indépendante de la machine. Pour les RPC de SUN Microsystems (ONC : « Open Network Computing ») ce protocole est appelé XDR (« eXternal Data Representation »). La figure 8 décrit l'empilement des différents protocoles. Cette figure montre comment s'insère le système de fichiers distribué NFS (« Network File system »).



*Figure 8 : empilement des protocoles jusqu'à NFS*

### VI.12 Les services de niveau supérieur

Cette partie est effectuée directement sur des machines UNIX, WINDOWS.

### VI.13 Exercices

#### Exercice 1

Modifier l'exemple de la section § V.7 afin d'utiliser le mode non connecté (SOCK\_DGRAM). Pour cela, au niveau du serveur il faudra créer la socket, la rattacher et, pour la réception des messages, utiliser la primitive suivante :

```
recvfrom(int s, char * buf, int leng, int flag, (struct sockadd *)&from, int fromlen).
```

Au niveau du client, il faudra créer la socket, la rattacher et, pour l'émission des messages, utiliser la primitive suivante :

```
sendto(int s, char * buf, int leng, int flag, (struct sockadd *)&to, int tolen).
```

## Exercice 2 : analyse de trames

frames à analyser :

00603E765E4A 0000C0B6DA9D 0806 00-01-08-00-06-04-00-01-00-00-C0-B6-DA-9D-C1-5F-11-43-00-00-00-00-00-00-C1-5F-11-01-00-01-63-5B-50-18-7C-00-0C-B7-00-00-2B-4F-4B-20-30-20-6F-32-00-00

00C0DF11EE65 00603E765E4A 0800 45-00-00-6A-53-22-40-00-EE-06-B0-96-82-E1-33-1E-C1-5F-11-76-00-15-04-23-7F-AA-41-06-69-D9-B3-84-50-18-22-38-E6-57-00-00-32-35-30-20-22-2F-6D-69-72-72-6F-72-73-2F-6C-69-71-75-6F-72-2E-63-61-62-69-2E-6E-65-74-2F-68-6F-6D-65-2F-6D-69-72-72-6F-72-2F-4A-44-4B-2D-31-2E-31-2E-33-22-20-69-73-20-6E-65-77-20-63-77-64-2E-0D-0A-74-75-65-2B

```
FFFFFFFFFFFF 00603E765E48 0800 45-00-00-35-00-00-00-00-FF-11-E8-D7-C1-5F-11-81-FF-FF-FF-
FF-18-49-00-45-00-21-00-00-00-01-65-6E-73-69-72-6F-75-74-65-72-2D-63-6F-6E-66-67-00-6F-63-74-
65-74-00-00-00-00-00
```

[illegible]

00C0DF11EE65 00603E765E48 0138 AA-AA-03-00-00-0C-20-00-01-B4-08-65-00-01-00-0E-65-6E-73-69-72-6F-75-74-65-72-00-02-00-27-00-00-00-02-01-01-CC-00-04-C1-5F-11-81-02-08-AA-AA-03-00-00-00-81-37-00-0A-00-00-00-01-00-60-3E-76-5E-48-00-03-00-0D-45-74-68-65-72-6E-65-74-30-00-04-00-08-00-00-00-01-00-05-00-D4-43-69-73-63-6F-20-49-6E-74-65-72-6E-65-74-77-6F-72-6B-20-4F-70-65-72-61-74-69-6E-67-20-53-79-73-74-65-6D-20-53-6F-66-74-77-61-72-65-20-0A-49-4F-53-20-28-74-6D-29-20-33-30-30-30-20-53-6F-66-74-77-61-72-65-20-28-49-47-53-2D-49-4E-2D-4C-29-2C-20-56-65-72-73-69-6F-6E-20-31-31-2E-30-28-39-29-2C-20-52-45-4C-45-41-53-45-20-53-4F-46-54-57-41-52-45-20-28-66-63-31-29-0A-43-6F-70-79-72-69-67-68-74-20-28-63-29-20-31-39-38-36-2D-31-39-39-36-20-62-79-20-63-69-73-63-6F-20-53-79-73-74-65-6D-73-2C-20-49-6E-63-2E-0A-43-6F-6D-70-69-6C-65-64-20-54-75-65-20-31-31-2D-4A-75-6E-2D-39-36-20-30-31-3A-31-35-20-62-79-20-6C-6F-72-65-69-6C-6C-79-00-06-00-0E-63-69-73-63-6F-20-32-35-30-30-00-00-00-00

00603E765E4A 0000C02DDB9D 0800 45-00-00-28-33-65-40-00-40-06-A0-39-C1-5F-11-42-CC-47-C8-48-79-4A-00-50-02-F2-2D-AB-A2-96-4D-6A-50-10-7C-00-32-6A-00-00-47-45-54-20-2F-69-2D-67-F2-72



Correspondance entre les LLC SAP et les noms

00	Management
02	Individual LLC sublayer management
06	Internet IP
42	IEEE 802.1d Spanning tree
AA	TCP/IP SNAP (Ethernet type in LLC)
E0	Novell IPX
F0	IBM NetBIOS
FF	Broadcast

Correspondance entre les numéros de protocole IP (en décimal) et les noms de protocoles

0	reserved
1	icmp, internet control message
2	igmp, internet group management
6	tcp
8	egp, exterior gateway protocol
9	igp, any interior gateway protocol
17	udp
29	iso-tp4
80	iso-ip

Types de trames Ethernet (en hexadécimal)

0800	DOD IP
0803	ECMA internet
0805	X.25 Level 3
0806	ARP
8137	Novell NetWare

Correspondance entre les 3 premiers octets d'une adresse MAC (en hexadécimal) et le nom du vendeur

00-00-C0	SMC
00-60-3E	Cisco
00-C0-DF	Kye Systems Corp
08-00-69	Silicon Graphics
08-00-6E	Excelan
00-20-AF	3Com

Correspondance entre les numéros de ports (en décimal) et les noms de service

13	daytime
53	domain
7	echo
69	tftp
79	finger
21	ftp
20	ftp-data
101	hostnames
25	smtp (mail)
23	telnet
79	finger
80	www
138	netbios-dg

Questions :

1. Quels sont les constructeurs des différentes cartes sur le réseau ?
2. Indiquer les différents empilements de protocoles que l'on observe à travers ces trames.

## **VI.14 Références**

- W. Stallings, Data and Computer Communications, 10<sup>th</sup> Edition, Pearson Education.
- I. Custer, « Au cœur de windows NT », Microsoft Press.
- J-L Montagnier, « Pratique des réseaux d'entreprise, du câblage à l'administration du réseau local aux réseaux télécom. », Eyrolles.
- R. Perlman, « Interconnection : bridges and routers », Addison-Wesley.
- G. Pujolle, Mschwartz, « Réseaux locaux Informatiques », Eyrolles.
- P. Rolin, « Réseaux locaux, normes et protocoles », Hermes.
- L. Toutain, « Techniques des réseaux locaux sous Unix », Hermes.
- L. Toutain, « Réseaux locaux et internet : des protocoles à l'interconnexion », Hermes.
- « Linux Network Administrator's Guide », O'Reilly Media.

