Chapitre 5

Les réseaux locaux d'entreprise

Pour répondre à leurs besoins propres en informatique distribuée, les entreprises ont mis en œuvre des *réseaux locaux d'entreprise*, constitués d'un ou plusieurs réseaux locaux ou LAN (*Local Area Network*). Ils utilisent des protocoles simples car les distances couvertes sont courtes (de quelques centaines de mètres à quelques kilomètres) et les débits importants (jusqu'à plusieurs centaines de Mbit/s). Après avoir vu la normalisation des architectures de réseaux locaux, nous détaillerons les différentes techniques d'accès au support, spécifiques de ce type de réseau. Puis nous analyserons le fonctionnement des réseaux locaux de première génération pour mieux comprendre leurs évolutions technologiques. Nous verrons comment interconnecter ces différents réseaux, en insistant sur les commutateurs qui occupent une place de choix dans les réseaux actuels. Enfin, nous aborderons les réseaux sans fil.

1 Architectures de réseaux locaux

Les réseaux locaux informatiques répondent aux besoins de communication entre ordinateurs au sein d'une même entreprise. Il s'agit de relier un ensemble de ressources devant communiquer : stations de travail, imprimantes, disques de stockage, ordinateurs, équipements vidéo. Nés dans les années 1970, ils ont été proposés par les fournisseurs informatiques. Leur « simplicité » et leur popularité sont dues au fait qu'ils furent conçus pour des environnements privés, sans recours aux solutions normalisées que proposaient les opérateurs de télécommunications (qui se trouvaient en situation de monopole à cette époque). L'accès à Internet fut ensuite largement facilité, du fait que les équipements étaient reliés au sein de l'entreprise. Il n'y avait plus qu'à mettre en place un partage sécurisé de cet accès.

Des réseaux plus étendus ont prolongé les réseaux locaux (surtout aux États-Unis) : des réseaux métropolitains ou interurbains appelés MAN (*Metropolitan Area Network*) se sont développés pour relier les établissements d'une même ville. Les réseaux grande distance ou WAN (*Wide Area Network*) assurent l'interconnexion de tous ces réseaux aux niveaux national et mondial. Des mécanismes d'interconnexion permettent de relier les réseaux locaux aux autres types de réseaux.

Un réseau local se caractérise par des équipements géographiquement proches les uns des autres et qui coopèrent en utilisant le support de transmission pour diffuser les données : l'ensemble des autres équipements du réseau reçoit tout bit émis par un équipement du réseau local. Cette particularité est à la base des architectures spécifiques de réseaux locaux, standardisées dans les années 1980. La section suivante nous permet de découvrir l'organisation physique des réseaux locaux, l'adressage, la topologie, le câblage et la couche Liaison de données.

1.1 Standards IEEE

Le comité 802 de l'IEEE, essentiellement constitué de représentants des constructeurs américains, s'est occupé de l'architecture des réseaux locaux. Plusieurs documents définissent l'architecture proposée (voir figure 5.1) :

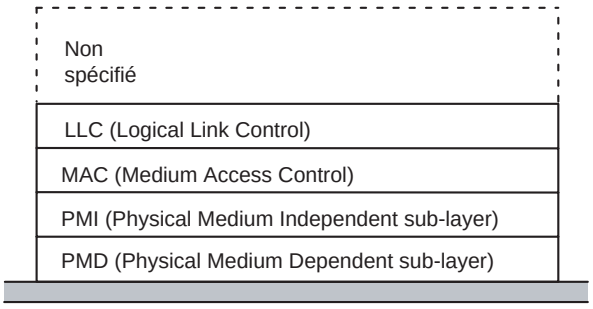
- Le standard 802.1 définit le contexte général des réseaux locaux informatiques.
- Le standard 802.2 définit la couche Liaison de données.
- Les standards 802.3, 802.4, 802.5 et 802.6 définissent différents protocoles d'accès au support, pour plusieurs types de supports physiques : paire métallique, câble coaxial ou fibre optique.
- Le standard 802.11 définit un protocole d'accès pour les réseaux locaux sans fil (WLAN, *Wireless LAN*).

D'autres standards ont vu le jour ultérieurement, au fur et à mesure de l'évolution technologique.

Par rapport au modèle OSI, l'architecture normalisée dans les réseaux locaux découpe la couche Liaison en deux sous-couches : MAC (*Medium Access Control*) et LLC (*Logical Link Control*). La première règle l'accès au support partagé. Elle filtre les trames reçues pour ne laisser passer que celles réellement destinées à l'équipement concerné. La seconde gère l'envoi des trames entre équipements, quelle que soit la technique d'accès au support. Les spécifications de l'IEEE ne concernent donc pas les couches situées au-dessus de LLC.

Figure 5.1

Modèle IEEE des réseaux locaux.



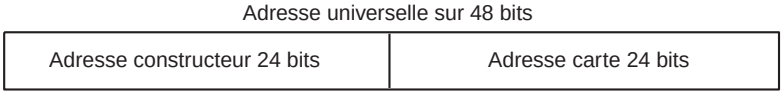
Comme on le voit à la figure 5.1, la couche physique est quelquefois découpée en deux niveaux : PMI (*Physical Medium Independent sub-layer*) qui assure le codage en ligne indépendamment du type de support de transmission utilisé, et PMD (*Physical Medium Dependent sub-layer*), qui s'occupe de l'émission physique du signal.

1.2 Adressage

Dans les réseaux locaux, l'adresse utilisée est une adresse physique qui se gère au niveau du matériel. Elle possède un format défini par l'IEEE sur 16 ou sur 48 bits. Ce dernier format constitue l'adressage universel des équipements : il correspond à un numéro de série dont un premier champ de 24 bits donne le constructeur de la carte (champ attribué par l'IEEE). Le second champ de 24 bits, librement choisi par le constructeur, est le numéro de la carte elle-même. De cette façon, toute carte réseau d'un ordinateur possède une adresse physique unique dans le monde[1]. Le format universel sur 48 bits est le plus utilisé (voir figure 5.2). Il est généralement baptisé *adresse MAC*, du nom de cette couche.

Figure 5.2

Format général des adresses MAC.



On peut également définir des adresses de groupe qui englobent plusieurs utilisateurs. Par exemple, dans le format universel, *l'adresse de diffusion* (ou *broadcast*) correspond à l'ensemble des équipements d'un réseau local. Dans cette adresse, tous les bits sont à 1. On l'écrit : `FF:FF:FF:FF:FF:FF` en hexadécimal.

Remarque

Les systèmes d'exploitation affichent l'adresse MAC de la carte réseau en hexadécimal, grâce à la commande `ifconfig` (pour Unix) ou `ipconfig` (pour Windows). On sépare les différents octets par deux points sous Unix ou par un tiret sous Windows, comme le montrent les deux exemples ci-après :
Sous Linux, la commande /sbin/ifconfig eth0 affiche (entre autres) :
eth0Link encap:EthernetHWaddr 00:90:27:6A:58:74
Sous Windows, la commande ipconfig /all affiche (entre autres) :
Adresse physique : 52–54–05-FD-DE-E5

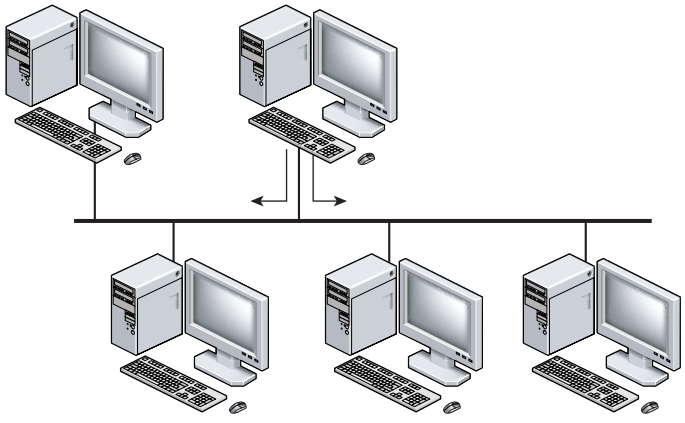
1. Cette règle n'est plus vraiment respectée, car il est désormais possible de programmer soi-même l'adresse MAC de sa carte réseau (voir l'explication dans la remarque de l'exercice 6).

À partir des trois topologies de base : le *bus*, l'*anneau* et l'*étoile*, de nombreuses versions sont possibles. Il faut distinguer la *topologie physique* de la *topologie logique*. La première caractérise la manière dont est réalisé le câblage du réseau local (la structure des chemins de câbles, le type de raccordement…) ; la seconde décrit comment on attribue le droit à la parole entre toutes les stations. La topologie logique définit la *méthode d'accès au support* (ou *niveau MAC*) utilisée.

Topologie physique

La *topologie en bus* consiste à utiliser un long câble, sur lequel les différents équipements se raccordent en série, pour qu'il n'y ait qu'un seul chemin sans boucle entre deux équipements du réseau local. Chaque station peut accéder à tout moment au support commun pour émettre. Les données sont diffusées à toutes les stations. Le temps de propagation n'étant pas nul, il peut se produire des *collisions* lorsque différentes stations émettent au même moment. L'exemple type d'une topologie en bus est illustré figure 5.3. Cette topologie permet de faire des communications point à point et se prête naturellement à la diffusion. En revanche, toute coupure du bus entraîne une panne complète du réseau.

Figure 5.3
Topologie en bus.



Dans la *topologie en anneau*, chaque station est connectée au support par un port d'entrée et transmet les données à la station suivante par son port de sortie. Les différentes stations sont reliées en cascade et les données circulent d'une station à l'autre, toujours dans le même sens : chaque station traversée prend le message, l'analyse puis le retransmet sur son port de sortie (voir figure 5.4).

L'anneau manque de fiabilité en cas de rupture du support. On le double parfois pour réaliser deux anneaux qui peuvent transmettre soit dans le même sens soit en sens inverse. La seconde solution est préférable car elle permet de reconstituer le réseau, même en cas de rupture des deux anneaux au même endroit.

La *topologie en étoile* est, en fait, la généralisation des liaisons point à point : chaque équipement est relié par une liaison spécifique à un équipement central. La complexité de celui-ci dépend des modes de communication entre stations. Cette topologie présente un point faible : le réseau est inutilisable en cas de panne de l'équipement central, lequel peut constituer un goulet d'étranglement et entraîner la dégradation des performances du réseau s'il est mal dimensionné.

Figure 5.4

Topologie en anneau.

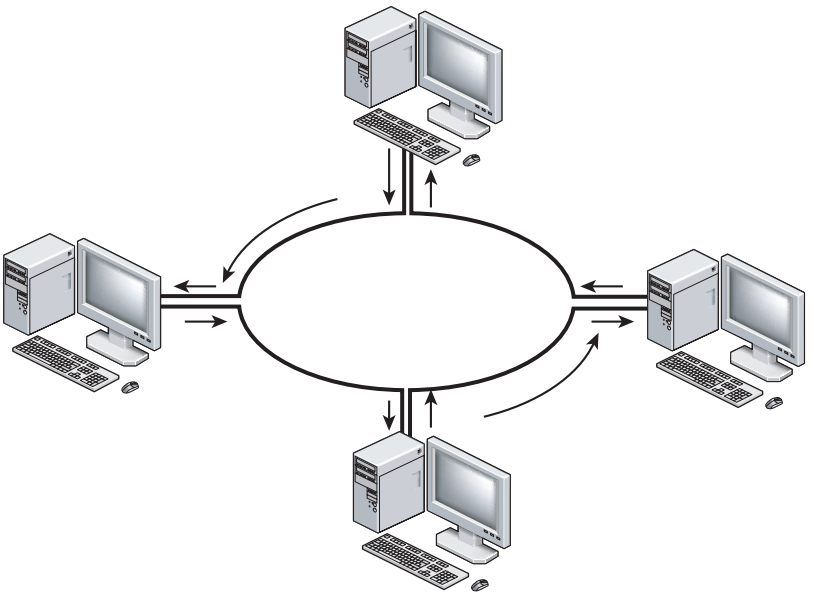
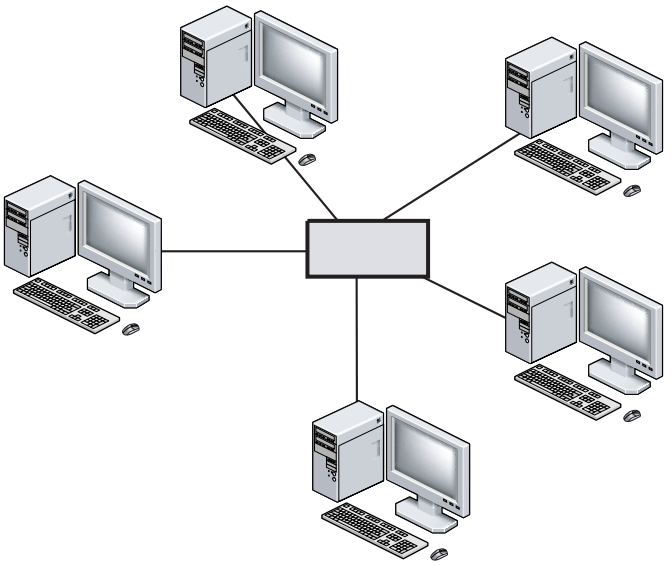


Figure 5.5

Topologie en étoile.



Topologie logique

La topologie logique s'appuie sur la manière dont les équipements échangent leurs données sur le réseau local. Elle ne dépend que du niveau MAC choisi et non de la façon de raccorder les équipements entre eux. Pratiquement, deux topologies logiques sont à considérer : le bus et l'anneau.

On peut en effet utiliser différentes topologies physiques pour réaliser une topologie logique donnée. Par exemple, une topologie logique en bus peut utiliser aussi bien un câblage physique en bus (cas du coaxial) qu'une topologie en étoile (pour un câblage physique par paires torsadées). De même, une topologie logique en anneau peut utiliser un anneau physique, un câblage en étoile autour d'un répartiteur, voire une topologie physique en bus !

1.4 Politique de câblage

La mise en place du câblage constitue un service de base, au même titre que l'infrastructure électrique des bâtiments. C'est pourquoi il faut disposer d'un système de câblage universel, adapté à la diversité des équipements et permettant la mise en œuvre de toutes les architectures de réseaux. Il existe deux possibilités de câblage : le *postcâblage* et le *précâblage*.

Le *postcâblage* consiste à installer l'infrastructure de communication, au fur et à mesure des besoins, dans des bâtiments qui n'avaient pas été prévus pour cela. On câble généralement le réseau local en calquant la topologie physique sur la topologie logique. L'accroissement du parc des équipements informatiques, les restructurations de sociétés, les déménagements donnent lieu à des modifications de câblage continuelles et coûteuses. Cette solution est de plus en plus obsolète.

Le *précâblage* se conçoit dès la construction du bâtiment. On le trouve aujourd'hui dans tous les bâtiments neufs, notamment dans les immeubles de bureaux. Il permet la mise en œuvre de toutes les topologies et consiste à poser une grande quantité de conducteurs offrant une grande souplesse d'arrangement. La présence des câbles est prévue à tous les étages, même si on ne connaît pas l'affectation future des locaux. Certains constructeurs proposent même une gestion technique du système de câblage. Le précâblage est évidemment moins coûteux pour l'entreprise.

1.5 Couche LLC

Le standard IEEE 802.2 définit un protocole de commande, LLC, fondé sur les principes du protocole normalisé HDLC que nous avons vu au chapitre 2. Trois classes sont définies :

- LLC1 fournit un service simple sans connexion ni contrôle, en point à point, en multipoint ou en diffusion.
- LLC2 assure un service avec connexion entre deux points d'accès et possède les fonctionnalités complètes du niveau Liaison du modèle OSI (contrôle de flux et contrôle d'erreur).
- LLC3, adapté au monde des réseaux industriels, rend un service sans connexion avec acquittement.

LLC1 est le protocole le plus courant dans les réseaux locaux informatiques. Il se réduit pratiquement à une seule trame : UI *(Unnumbered Information)*, trame d'information non numérotée, correspondant à la notion de datagramme. Le service rendu par le protocole LLC1 est minimal : il se contente de formater les messages à émettre et de leur ajouter un bloc de contrôle d'erreur. Le récepteur vérifie le bloc de contrôle et détruit les messages reçus erronés. Il n'y a aucun accusé de réception, ni aucune demande de retransmission. Un tel fonctionnement est acceptable dans l'environnement des réseaux locaux car les distances ainsi que les taux d'erreur sont très faibles. Les messages manquants sont éventuellement détectés puis réémis au niveau de la couche Transport.

LLC2 est un protocole complet, analogue à la norme HDLC vue au chapitre 2. Quant à LLC3, il ajoute à LLC1 la notion d'accusé de réception. Dans les réseaux locaux industriels ou la commande de processus, il est important de garantir la fiabilité des transmissions, d'où l'idée d'un protocole sans connexion qui permette la bonne réception des messages sans la lourdeur imposée par la gestion des connexions.

Les trois classes de LLC étaient destinées à couvrir l'ensemble des besoins des utilisateurs. Aujourd'hui, la plupart des installations existantes se contentent de LLC1.

2 Techniques d'accès au support

Les réseaux locaux nécessitent un partage du support – donc de sa bande passante utile – entre les différents utilisateurs. Les constructeurs informatiques ont proposé de nombreuses techniques d'accès regroupées en deux grandes familles : les unes *à accès aléatoire*, les autres *à accès déterministe*.

Dans les techniques à accès aléatoire, chaque équipement émet ses données sans se soucier des besoins des autres. Plusieurs variantes sont fondées sur ce principe.

Dans les techniques déterministes, l'accès au support se fait à tour de rôle. L'accès est soit fixé *a priori* (indépendamment de l'activité des équipements), soit dynamiquement (en fonction de leur activité). Cette famille de techniques comprend tous les protocoles à *jetons*, dans lesquels le droit d'émettre est explicitement alloué à un équipement grâce à une trame particulière appelée *jeton*.

Remarque

Aloha, la plus ancienne méthode de contrôle d'accès à un support physique, appartient aux techniques aléatoires. Elle consiste à envoyer un message, sans s'occuper de ce que font les autres équipements. En cas de collision, le message est retransmis au bout d'un temps aléatoire. Son nom provient de l'archipel d'Hawaï car cette technique y fut expérimentée pour la première fois, dans un réseau hertzien reliant les différentes îles.

2.1. Techniques d'accès aléatoire

Les méthodes d'accès aléatoire portent le nom générique de CSMA (*Carrier Sense Multiple Access)*. Elles sont bien adaptées à la topologie en bus et exploitent la très faible distance entre les équipements. Quand un équipement a une trame à émettre, il se met à l'écoute du support[2], attend que celui-ci soit libre avant de commencer la transmission. Du fait des temps de propagation non nuls, un équipement peut provoquer une collision, même s'il a écouté au préalable et n'a rien entendu : plus le délai est grand et plus le risque de collision augmente.

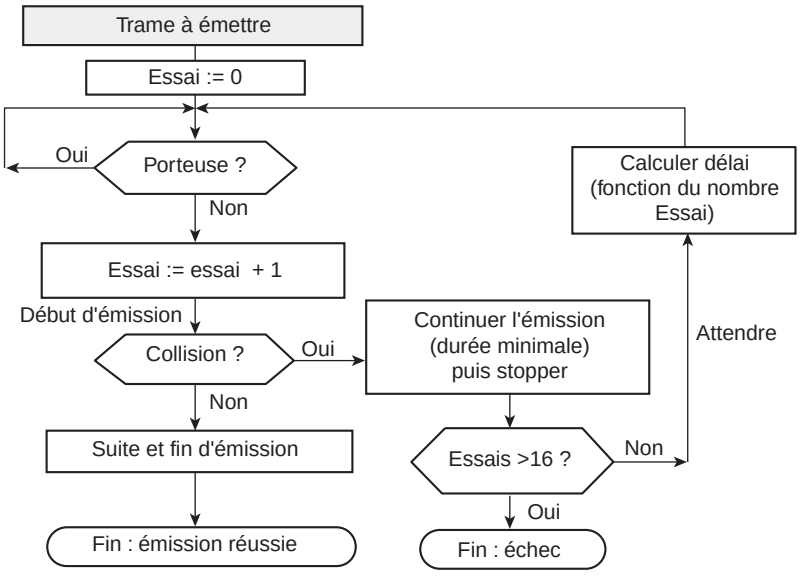
Il existe différentes variantes de ce mécanisme. La plus classique est normalisée sous le nom IEEE 802.3 : CSMA/CD (*CSMA with Collision Detection*). L'originalité de ce mécanisme, illustré à la figure 5.6, est que l'équipement *continue* d'écouter le support de transmission après le début de son émission. Il *arrête d'émettre*, après un très bref délai, s'il détecte une collision[3]. Le temps d'écoute pendant l'émission est limité à quelques microsecondes (il représente le temps de propagation aller et retour entre les deux stations les plus éloignées). La durée de la collision est ainsi réduite au strict minimum. La période pendant laquelle il est impossible d'éviter une collision malgré l'écoute préalable s'appelle *période de vulnérabilité*. La longueur maximale du bus détermine la durée maximale de cette période.

2. « Écouter » revient à mesurer la puissance du signal reçu : en effet, le rapport signal/bruit garantit qu'on sait faire la différence entre un signal de données et un simple bruit sur le support. Le support est libre si on ne détecte pas de signal transportant une donnée.

3. Lorsque deux stations émettent simultanément, leurs signaux se superposent et chaque émetteur ne reconnaît plus son message sur le support.

Figure 5.6

Mécanisme CSMA/CD.



Avec une technique aléatoire, le temps nécessaire pour émettre une trame ne peut être garanti. En effet, les retransmissions sont faites au bout d'un intervalle de temps qui dépend du nombre de tentatives. Après 16 tentatives infructueuses, l'équipement abandonne. L'intérêt de cette technique est sa simplicité de mise en œuvre, car elle ne nécessite pas la présence d'un équipement de contrôle. De plus, elle est totalement décentralisée, indépendante du nombre et de l'état des machines connectées.

2.2. Techniques d'accès déterministe

Les techniques déterministes utilisent un *jeton,* sur un bus ou sur un anneau. Le jeton est une trame qui circule dans le réseau d'équipement en équipement : un équipement *A* qui reçoit et reconnaît le jeton possède « le droit à la parole ». Il est autorisé à émettre sur le support (voir figure 5.7). Une fois sa transmission terminée, il transmet le jeton à l'équipement suivant. Le mode de transmission du jeton dépend de la topologie logique du réseau :

- Dans un anneau, l'équipement suivant est le premier équipement opérationnel, physiquement relié au précédent et en aval de celui-ci. La transmission du jeton (ou de toute trame) se fait toujours vers cet équipement, sans qu'il y ait besoin de le désigner explicitement : le jeton est *non adressé*.
- Dans un bus, l'équipement suivant est l'un des équipements du réseau, connu seulement du possesseur du jeton. Une trame contenant le jeton est diffusée sur le bus et possède l'adresse explicite du destinataire ou *successeur*. Chaque équipement n'a qu'un et un seul successeur dont il connaît l'adresse. On crée ainsi un *anneau virtuel* de circulation du jeton. Le jeton est *adressé*.

En fonctionnement normal, une phase de transfert de données alterne avec une phase de passation du jeton. Chaque équipement doit pouvoir traiter la réception et le passage du jeton, en respectant le délai maximal défini par la méthode d'accès. Il est également indispensable de prendre en compte l'ajout d'un nouvel équipement. Enfin, il faut réagir à l'altération, voire à la perte du jeton (cette trame, comme les autres, peut subir des erreurs de transmission) en mettant en place un mécanisme de *régénération* du jeton qui dépend du type du jeton (adressé ou non).

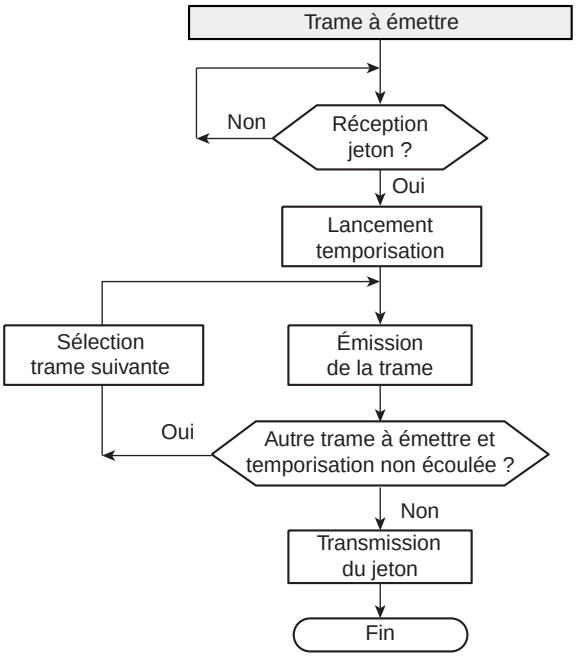


Figure 5.7
Mécanisme de jeton.

Pour mieux comprendre le fonctionnement des réseaux locaux, nous allons décrire les réseaux de première génération (*Ethernet*-IEEE 802.3 et *Token Ring*-IEEE 802.5). Ils diffèrent par leur organisation physique, leurs supports, leur plan de câblage, ainsi que par le format des trames. Nous verrons à la section 5 comment ces réseaux ont évolué au cours des trente dernières années.

3 Ethernet IEEE 802.3 de première génération

La société Xerox a développé Ethernet en 1976. Ce fut le premier produit de réseau local utilisant le mécanisme CSMA/CD sur un bus physique. Vu son grand succès, les sociétés Xerox, DEC et Intel ont décidé d'en faire un standard qui a servi de base au comité IEEE pour sa norme 802.3, même si Ethernet et le standard IEEE 802.3 diffèrent sur des points mineurs. La réussite d'Ethernet a été considérable : il est d'usage courant maintenant d'appeler Ethernet tout réseau local utilisant CSMA/CD, même s'il n'a plus grand-chose en commun avec le réseau initial.

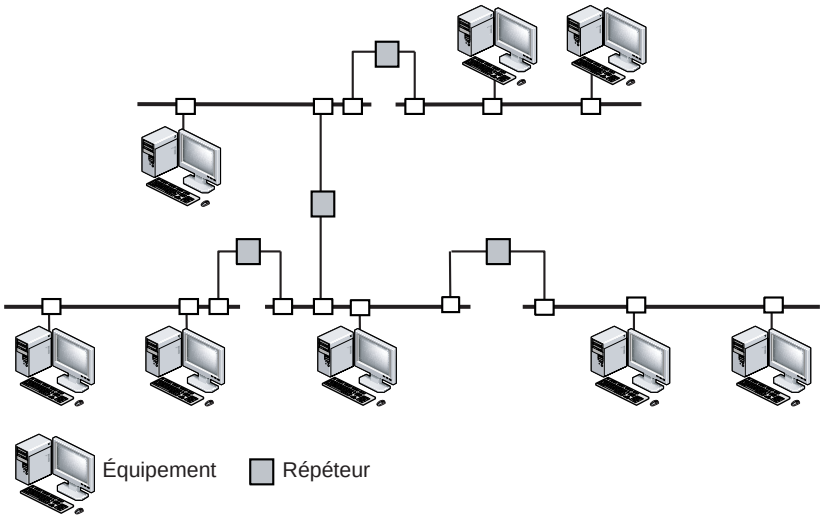
3.1 Organisation physique d'un réseau Ethernet

Les réseaux IEEE 802.3 utilisent une transmission en bande de base avec un code Manchester. Le réseau est organisé en un ou plusieurs segments, reliés de façon à conserver la structure de bus (voir figure 5.8). Afin que tous les équipements reçoivent un signal de puissance suffisante, la longueur de chaque segment est limitée. Pour des longueurs supérieures, il faut utiliser des *répéteurs*, qui décodent et amplifient les signaux reçus sans les interpréter. Ils contribuent à augmenter légèrement le délai de propagation et relient différents segments de façon à former un seul bus logique et un seul *domaine de collision* (ensemble des stations susceptibles de provoquer des collisions en cas d'émissions simultanées).

Pour limiter les risques de collision, le standard impose un délai de propagation aller et retour du signal strictement inférieur à 51,2 microsecondes.

Figure 5.8

Structure de bus « ramifié ».



Remarque

Chaque extrémité d'un bus est munie d'un *bouchon de terminaison* qui est, en fait, une résistance électrique dont l'impédance est égale à 50 Ω (impédance caractéristique du bus). Son rôle est d'absorber le signal électrique qui se propage, pour l'empêcher au maximum d'être réfléchi à l'extrémité du support et provoquer par là un brouillage du signal par lui-même. Le bouchon d'extrémité joue un rôle important dans la structure du réseau, puisqu'il absorbe littéralement le message émis sous la forme d'un courant électrique.

3.2 Format de la trame Ethernet

La figure 5.9. illustre le format de la trame Ethernet de base. Il comprend un long préambule (`101010`…) provoquant l'émission d'un signal rectangulaire de fréquence 10 MHz si le débit de transmission est de 10 Mbit/s. L'ensemble des équipements du réseau se synchronise ainsi sur le message émis. Le champ SFD (*Start Frame Delimitor)* contient la séquence `10101011` qui marque le début de la trame.

La trame contient dans son premier champ significatif l'adresse du destinataire DA (*Destination Address*) et celle de l'expéditeur SA (*Source Address*). Il s'agit des adresses MAC dont nous avons parlé à la section 1.2. Un champ sur deux octets précise la longueur (en nombre d'octets) des données de la couche LLC. La norme 802.3 ayant défini une longueur minimale de trame à 64 octets (qui représente à 10 Mbit/s un temps de transmission de 51,2 microsecondes), celle-ci est complétée par des octets de « bourrage » si la trame est plus courte. En fait, la taille de la trame doit être comprise entre 64 et 1 518 octets, ce qui laisse de 46 à 1 500 octets « utiles » dans le champ de données. La taille maximale est imposée pour assurer un rôle équitable entre les différents équipements (celui qui a réussi à prendre la parole ne peut pas la monopoliser…). La trame se termine par un champ FCS (*Frame Check Sequence)*. Calculé par l'émetteur, le FCS permet au

récepteur de vérifier la validité des trames reçues. La détection des erreurs se fait à l'aide du polynôme générateur :

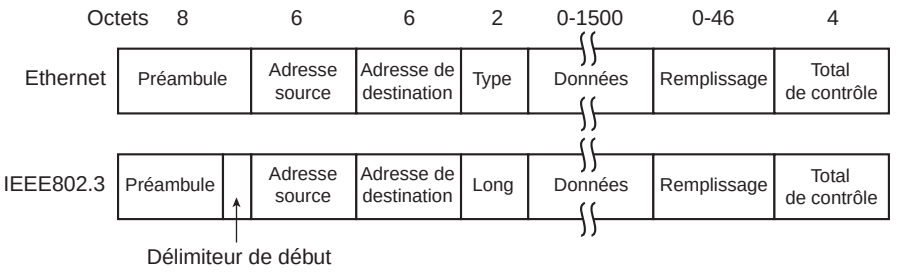
$$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^5 + x^4 + x^2 + 1.$$

Une trame doit contenir obligatoirement un nombre entier d'octets. Enfin, un silence, obligatoire entre les trames, dure 9,6 microsecondes.

Figure 5.9

Format de la trame Ethernet.

(a) Ethernet
(b) IEEE802.3



Initialement, dans la norme IEEE 802.3, le champ longueur devait indiquer la longueur réelle du contenu de la trame. Dans la pratique, le contenu de la trame définit implicitement sa propre longueur. Ce champ, rebaptisé *type*, s'utilise désormais pour indiquer à quel protocole appartiennent les données encapsulées dans la trame. Par exemple, il peut prendre (en hexadécimal) les valeurs suivantes : `0800` (protocole IP), `0806` (protocole ARP), `0835` (protocole RARP). Nous reverrons au chapitre 6 le rôle de ces trois protocoles.

3.3 Supports et plan de câblage d'Ethernet

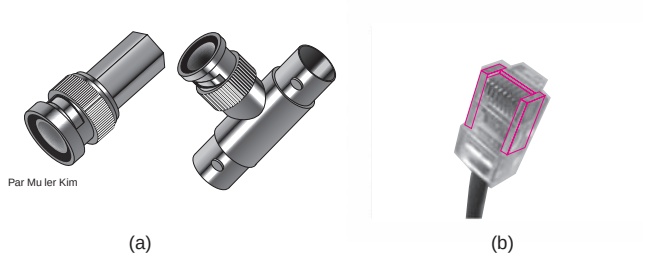
Historiquement, la première solution rencontrée est un plan de câblage en bus et le support utilisé un câble coaxial. Les équipements raccordés doivent respecter entre eux une contrainte de distance minimale. La nomenclature, sous la forme *XBase n*, décrit le débit du réseau et le support : *X* exprime le débit en Mbit/s, *Base* indique une transmission en bande de base, et *n* renseigne sur le type de câble. Les câblages initialement utilisés sont le *10 Base 5* et le *10 Base 2* :

- 10 Base 5 est un câble coaxial de 500 m maximum par segment, avec une transmission en bande de base et un débit de 10 Mbit/s. Il est à l'origine du produit Ethernet.
- 10 Base 2 est un câble coaxial plus fin donc plus maniable, de 180 m maximum par segment, avec une transmission en bande de base et un débit de 10 Mbit/s.

Le câble est posé dans des goulottes et alimente les différents bureaux. Le raccordement physique de la station au coaxial utilise une prise BNC (voir figure 5.10). Si le branchement d'un nouvel équipement est très facile à pratiquer, ce type de câblage présente toutefois deux inconvénients : la longueur maximale est facilement atteinte dans un bâtiment, et la coupure du bus empêche le fonctionnement du réseau.

Figure 5.10

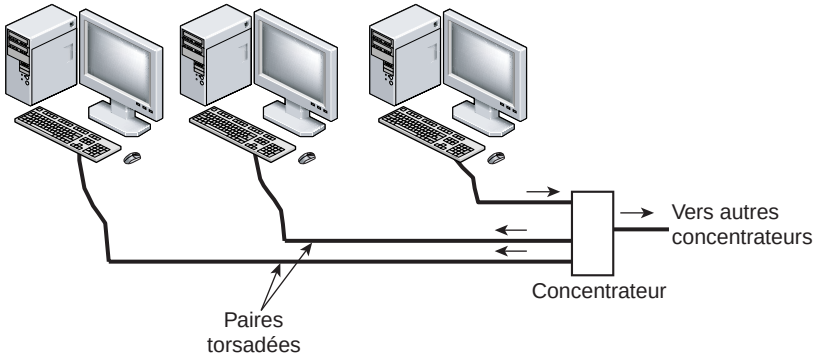
Connecteurs (a) BNC et (b) RJ45.



Dès les années 1990, on a recours au câblage en étoile (voir figure 5.11), dans lequel toutes les stations sont branchées sur un « concentrateur », ou *hub*, qui retransmet sur l'ensemble de ses ports tout signal reçu sur un port quelconque. La topologie logique reste celle d'un bus et le fonctionnement de l'accès par CSMA/CD est inchangé. Le support le plus courant fut alors la paire torsadée : 10 Base T (T pour *Twisted pair*) est une paire torsadée de 100 m par segment, transmettant en bande de base à un débit de 10 Mbit/s. La prise RJ45 remplace dans ce cas le connecteur BNC (voir figure 5.10). On peut aussi utiliser une fibre optique 10 Base F (*F* pour *Fiber*) de 2,5 km, transmettant en bande de base à 10 Mbit/s. Certains concentrateurs ont plusieurs ports pour raccorder des paires torsadées et un port pour raccorder une fibre optique, par exemple.

Figure 5.11

Câblage en étoile autour d'un concentrateur (hub).



Le concentrateur reste un équipement qui agit exclusivement au niveau du signal transmis : si la nature des supports change entre ses ports, il est simplement capable de récupérer les données binaires et d'en refaire le codage. Il n'interprète en aucun cas les données reçues.

3.4 Conclusion sur Ethernet

La grande force du standard IEEE 802.3 est sa simplicité : il n'y a aucun équipement centralisant le contrôle du réseau. L'ajout et le retrait d'un équipement se font sans interruption de fonctionnement, que ce soit avec un câblage en bus ou en étoile sur le concentrateur. Si le trafic est faible, l'accès au support est quasiment immédiat. En revanche, le réseau supporte mal les fortes charges qui peuvent provoquer un effondrement du débit utile, car le temps d'accès au support n'est pas borné. Un réseau 802.3 est donc une solution rapide et peu coûteuse à mettre en œuvre, destinée principalement à la bureautique. Les concentrateurs rassemblent en un point tous les raccordements physiques, ce qui améliore la sécurité et la rapidité d'intervention en cas de panne.

4 Token Ring IEEE 802.5

La société IBM a développé l'anneau à jeton ou Token Ring, standardisé par l'IEEE sous le nom 802.5. Les développements datent de la même époque qu'Ethernet mais les solutions proposées sont totalement différentes, tant dans l'organisation physique que dans le format des trames et les supports utilisés.

4.1 Organisation physique de l'anneau à jeton

La transmission se fait en bande de base avec un code Manchester différentiel (au lieu de coder chaque bit, le codage différentiel code la différence entre deux bits consécutifs). La topologie physique est un anneau simple unidirectionnel, dans lequel un équipement opérationnel actif sur l'anneau répète ce qu'il reçoit de l'amont vers l'équipement en aval. Un équipement en panne ou éteint ne participe pas à l'anneau (on dit qu'il est mis en *by-pass*) mais la propagation du signal est assurée. Des dispositifs électroniques ou électromagnétiques permettent à l'anneau de se reconfigurer automatiquement en cas d'incident.

À chaque instant, on distingue deux types d'équipements dans le réseau : celui qui « possède » le jeton et les autres. La topologie logique est un anneau dans lequel un équipement qui n'a pas le jeton se comporte comme un simple répéteur physique. L'équipement qui détient le jeton a le droit d'émettre une trame vers son successeur qui la transmet au suivant et ainsi de suite jusqu'à l'équipement émetteur. Celui-ci peut donc vérifier, en comparant la trame reçue avec la trame émise, que celle-ci a correctement fait le tour de l'anneau. Il peut savoir si le destinataire l'a correctement reçue et recopiée. Lorsqu'un équipement a fini de recevoir sa propre trame, il émet la trame spéciale contenant le jeton et repasse en fonctionnement de base.

4.2 Format de la trame 802.5

La figure 5.12 illustre le format des trames 802.5. Lorsqu'il n'y a aucun trafic de données, le jeton circule dans l'anneau d'un équipement à l'autre. Il faut que la durée *t* entre l'émission d'un élément binaire et sa réception après un tour complet de l'anneau soit supérieure à la durée d'émission du jeton. On appelle *latence de l'anneau* la quantité d'informations qu'il contient à un instant donné. La latence doit être supérieure à la durée d'émission d'une trame de jeton codée sur 24 bits. Si l'anneau est trop court, l'équipement de surveillance ou *moniteur* (*Monitor*) gère une petite mémoire tampon pour retarder la répétition du signal et porter la latence à 24 bits.

Le champ SD (*Start Delimitor*) marque le début d'une trame. AC (*Access Control*) indique s'il s'agit d'une trame « jeton libre » ou d'une trame de données. En outre, cet octet contient un bit *M* géré par le moniteur et deux groupes de 3 bits, donnant respectivement la priorité du jeton (ou de la trame transmise) et la priorité des trames en attente dans les stations de l'anneau. FC (*Frame Control*) donne le type de la trame. Les champs d'adresses MAC (DA, SA) et le bloc de contrôle d'erreurs (FCS) sont définis comme dans IEEE 802.3. L'octet ED (*End Delimitor)* délimite la fin du jeton ou de la trame de données. Dans cette dernière, ED est suivi d'un octet FS (*Frame Status)* qui véhicule des informations de contrôle.

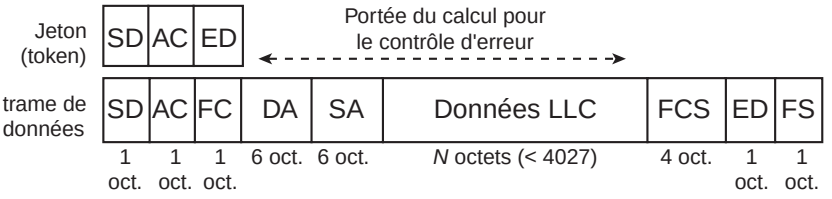


Figure 5.12
Format de la trame 802.5.

FS contient deux indicateurs (répétés par sécurité dans la seconde moitié de l'octet) : ARI (*Address Recognized Indicator*, ou indicateur d'adresse reconnue) et FCI (*Frame Copied Indicator*, ou indicateur de trame copiée). ARI est mis à 1 quand le récepteur reconnaît son adresse. FCI, quant à lui, est mis à 1 si le récepteur est parvenu à copier avec succès la trame provenant de l'anneau.

Les délimiteurs de début et de fin (SD et ED) sont des séquences particulières qui violent le principe du code Manchester : certains symboles de l'octet ne correspondent ni à un 0 ni à un 1 valides (on parle parfois de « non-données »).

4.3 Gestion de l'anneau

L'équipement détenteur du jeton peut émettre une trame qui fait le tour de l'anneau avant de lui revenir. Grâce aux différents indicateurs, l'équipement vérifie que l'anneau n'est pas coupé, qu'il n'y a qu'un seul moniteur actif et que le destinataire a bien copié la trame. Il détecte aussi la demande de jeton de plus haute priorité exprimée par un autre équipement du réseau. Après avoir reçu correctement sa propre trame, il émet un jeton libre sur l'anneau.

Pour éviter toute utilisation abusive du support, chaque station arme un temporisateur au début de la phase d'émission. Elle passe obligatoirement le jeton lorsque ce temporisateur expire, ce qui revient à déterminer la taille maximale d'une trame. On peut aussi affecter différentes priorités aux équipements du réseau. Celui qui a une trame en attente de priorité inférieure à celle du jeton ne peut prendre le jeton circulant. Il doit attendre le passage d'un jeton doté d'une priorité inférieure ou égale à celle de sa trame.

La mise hors service ou la panne de l'équipement qui possédait le jeton provoque la disparition de celui-ci. Un anneau à jeton est donc compliqué à surveiller : le moniteur crée un jeton à l'initialisation de l'anneau, surveille l'activité des équipements connectés, régénère le jeton en cas de perte, détecte les messages ayant fait plus d'un tour, assure la synchronisation bit, ajuste la latence de l'anneau, etc. En outre, pour remplacer le moniteur actif quand celui-ci tombe en panne, tous les autres équipements jouent le rôle de *moniteurs dormants* (*Standby Monitor*)…

Tant que le moniteur est opérationnel, il doit envoyer à intervalles réguliers une trame AMP (*Active Monitor Present*). Dès que cette trame n'est plus envoyée en temps voulu, une des stations dormantes émet une trame *Claim Token* pour prendre le contrôle de l'anneau. Si elle y parvient, elle devient le moniteur actif. Les stations dormantes signalent leur présence à intervalles réguliers en transmettant la trame SMP (*Standby Monitor Present*).

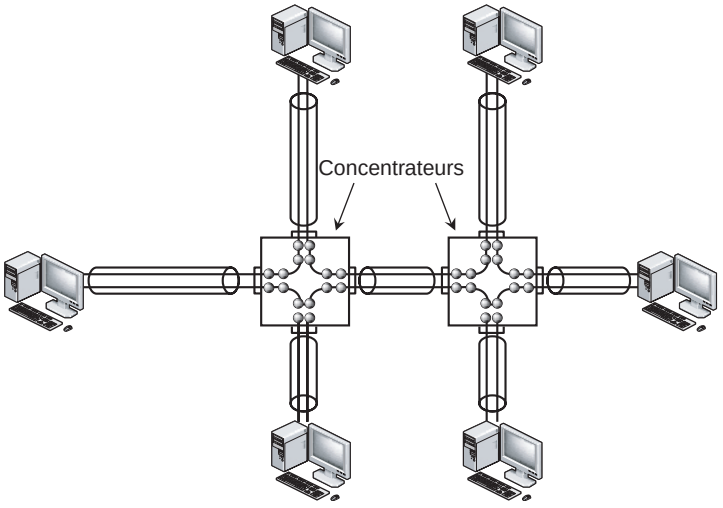
L'échange de trames AMP-SMP s'utilise également pour déterminer la liste des stations actuellement opérationnelles dans le réseau. Pour cela, le moniteur envoie une trame AMP et utilise l'adresse de diffusion générale (*broadcast address*) dans le champ adresse destination. Chaque station active de l'anneau propage le jeton libre engendré par la station la plus proche du moniteur. Elle émet une trame SMP contenant l'adresse de diffusion générale comme adresse destination et sa propre adresse comme adresse source (NAUN, *Nearest Active Upstream Neighbour*). La procédure se poursuit jusqu'à ce que toutes les stations actives de l'anneau aient répondu. À son retour dans le moniteur, la trame SMP contient l'adresse de son voisin aval, situé le dernier sur l'anneau.

Cette procédure est importante en cas de défaillance partielle ou totale de l'anneau. Si une station ne reçoit pas le flot de bits entrants, elle envoie une trame d'alarme *Beacon* pour signaler une condition d'erreur possible aux stations aval et au moniteur. Dans cette trame, la présence du champ NAUN facilite le diagnostic d'erreur.

4.4 Supports et plan de câblage

Le plan de câblage généralement proposé pour l'anneau à jeton est une étoile ou un ensemble d'étoiles. Un concentrateur actif AWC (*Active Wire ring Concentrator*) permet de constituer l'anneau (voir figure 5.13). Par des dispositifs électroniques ou électromécaniques, AWC surveille la présence active de chaque équipement (détection d'un équipement hors tension, d'un câble coupé…) et reconfigure l'anneau automatiquement en cas d'incident, en excluant l'équipement concerné (mise en *by-pass*). Il est possible de relier plusieurs concentrateurs entre eux pour augmenter la taille de l'anneau et le nombre des stations.

Figure 5.13
Câblage en étoile d'un anneau.



Le câble de raccordement entre l'équipement et le concentrateur est généralement une paire torsadée blindée d'impédance 150 Ω. Les débits possibles sont de 1 ou 4 ou 16 Mbit/s. Le nombre de stations dans l'anneau peut dépasser 200.

4.5 Conclusion sur l'anneau à jeton

Le débit utile d'un anneau résiste bien à la charge et ne s'effondre jamais comme avec la norme IEEE 802.3. Comme le délai d'accès au support est borné, on peut mettre en œuvre des dialogues entre équipements sur lesquels s'exécutent des applications temps réel. L'inconvénient principal de l'anneau à jeton réside dans la lourdeur et la complexité des mécanismes de sa gestion. Un tel réseau est donc globalement plus coûteux qu'un réseau Ethernet. Paradoxalement, les performances de l'anneau à jeton sont pénalisées à faible charge : le délai d'accès étant non nul, il faut attendre le jeton avant d'émettre alors que l'accès est immédiat en CSMA/CD sur un bus libre. De ce fait, l'anneau à jeton n'a pas pu offrir des débits supérieurs à 16 Mbit/s et n'a pu suivre l'accroissement des débits disponibles sur les réseaux Ethernet.

5 Évolution des réseaux locaux

Si Ethernet a été initialement conçu pour fonctionner sur des câbles coaxiaux à un débit de 10 Mbit/s, il est devenu le réseau local le plus répandu, dès qu'on a pu utiliser le câblage téléphonique et les paires métalliques. Deux évolutions majeures ont eu lieu simultanément :

l'utilisation de débits plus élevés et l'apparition des commutateurs. Enfin, l'avancée technologique a permis l'avènement des réseaux sans fil dont le développement est en plein essor, en raison du confort de raccordement qu'ils procurent.

5.1 Fast Ethernet, Ethernet commuté, Gigabit Ethernet

Fast Ethernet est une version d'Ethernet à 100 Mbit/s compatible avec les réseaux à 10 Mbit/s. Elle a été largement diffusée dès le milieu des années 1990. Les concentrateurs proposés étaient bien souvent compatibles 10 et 100 Mbit/s. Ils se différenciaient simplement par leur nombre de ports. Gigabit Ethernet est la version à 1 Gbit/s (1 000 Mbit/s, standard 802.3z) qui a suivi. Les équipements Gigabit combinent généralement des ports à 10 et 100 Mbit/s avec une ou plusieurs connexions sur des fibres optiques à 1 Gbit/s. La paire métallique non blindée de catégorie 5 peut, elle aussi, supporter le débit de 1 Gbit/s sur de courtes distances. Une version Ethernet 10 Gbit/s est apparue en 2001 (Standard 802.3ae).

La fibre optique la plus utilisée est la fibre multimode. Dans ce support, un transducteur optique assure la transformation entre le signal lumineux et le signal électrique. La distance maximale entre deux équipements est de 1,5 km. Les nouvelles technologies issues des recherches les plus récentes promettent des fibres multifréquences (1 024 canaux par fibre) avec, pour chaque canal, un débit de plusieurs Go/s. Le principal désavantage de la fibre est son coût élevé.

Parallèlement, les concentrateurs ont été remplacés par des commutateurs (*switches*). Dans un réseau Ethernet commuté, tous les équipements du réseau sont reliés à un (ou plusieurs) commutateurs. La topologie physique peut être mixte : en étoile pour toutes les stations directement connectées au commutateur, en bus pour celles qui sont reliées *via* un concentrateur. Le commutateur, à la différence du concentrateur, lit les trames qu'il reçoit et exploite l'adresse du destinataire : il ne transmet la trame que sur le port qui permet d'atteindre le destinataire et non sur tous les ports. Si le port est occupé, le commutateur mémorise la trame et attend que ce dernier se libère. De plus, il possède des ressources de traitement élevées et peut gérer plusieurs trames simultanément. Il accroît donc énormément la capacité du réseau *:* par exemple au lieu de partager un débit de 100 Mbit/s entre tous les équipements reliés par un concentrateur, on obtient 100 Mbit/s dédiés à chacun d'entre eux dès lors qu'ils sont reliés par un commutateur : s'il y a 10 équipements dans le réseau dialoguant deux à deux, on peut obtenir un débit global de 500 Mbit/s.

Gigabit Ethernet s'est développé dans les environnements commutés et possède deux modes de fonctionnement : les modes *duplex intégral* et *semi-duplex*. Dans le mode duplex intégral, utilisé sur les liaisons point à point, un équipement émet et reçoit simultanément des données avec le commutateur ; il n'y a plus de collision possible. Le semi-duplex est employé pour les équipements raccordés par l'intermédiaire d'un concentrateur. Dans ce cas, des collisions peuvent encore se produire.

Grâce au débit employé, le temps d'émission d'une trame est très faible. Il a fallu apporter des fonctionnalités supplémentaires dans la méthode d'accès : l'*extension de trame* et le *mode rafale*. La première consiste à porter la longueur minimale de la trame à 512 octets (au lieu de 64 octets dans l'Ethernet classique) ; la seconde permet à un émetteur d'envoyer en une seule fois plusieurs trames consécutives. Ces deux fonctionnalités rendent supportable la contrainte de longueur maximale du réseau.

Il existe principalement deux technologies de commutateurs : *store and forward* et *cut through*. Quand un commutateur store and forward reçoit une trame, il la vérifie et, si elle ne possède pas d'erreurs, la stocke avant de l'envoyer sur le port adéquat. Ce fonctionnement convient bien au mode client/serveur car il élimine les trames erronées et accepte le

mélange de divers supports (cuivre-fibre optique, par exemple) ou encore le mélange de débits. Il présente l'inconvénient d'introduire un délai supplémentaire, puisque chaque trame est transmise deux fois. Un commutateur cut through analyse l'adresse MAC du destinataire et transmet la trame à la volée sans aucune vérification. Ce système fournit de faibles temps d'attente, mais il n'apporte aucun service à valeur ajoutée puisque même les trames incomplètes sont transférées. Une variante adaptative consiste à mesurer le taux d'erreur pendant le fonctionnement cut through et à basculer en store and forward si ce taux dépasse un certain seuil.

Enfin, les commutateurs peuvent intégrer des fonctions supplémentaires pour gérer, par exemple, une table de correspondance adresses MAC-numéros de ports sur plusieurs commutateurs reliés entre eux. On gère les commutateurs par une interface locale ou une interface Web.

5.2 Réseaux locaux virtuels ou VLAN (Virtual LAN)

L'introduction des commutateurs dans un réseau local a permis de construire des réseaux logiques, indépendants les uns des autres. Les réseaux sont désormais définis en fonction des centres d'intérêt de leurs utilisateurs, et non en fonction de la situation géographique des équipements au sein de l'entreprise. On parle alors de *réseaux locaux virtuels* ou VLAN (*Virtual LAN*).

Un réseau virtuel regroupe une communauté d'usagers répartis dans toute l'entreprise, comme s'ils appartenaient au même réseau physique. Les échanges à l'intérieur d'un VLAN sont sécurisés et les communications entre VLAN contrôlées. Par exemple, le réseau virtuel réservé à la direction de l'entreprise fournit un espace de communication sécurisé à l'équipe directoriale. Ce réseau est logiquement distinct du réseau virtuel affecté aux services de production, même si les machines des deux départements sont reliées physiquement aux mêmes commutateurs.

On utilise plusieurs techniques de différentiation des équipements pour créer un VLAN. La première opère au niveau des ports du commutateur : un sous-ensemble des ports correspond à un VLAN donné. Cette solution a l'inconvénient de ne pas gérer la mobilité des utilisateurs. La deuxième consiste à identifier les équipements d'un VLAN par leurs adresses MAC, quel que soit le port du commutateur sur lequel l'équipement est raccordé. Cette solution est plus souple que la précédente, mais elle lie encore l'appartenance à un VLAN particulier au matériel utilisé. La troisième utilise les adresses IP, nous la verrons au prochain chapitre.

Le commutateur contient une table de correspondance entre les VLAN et la liste des ports associés. Pour gérer le VLAN avec un maximum de souplesse (quelle que soit la technique de différentiation), il faut qu'il soit étiqueté (*tagged*), c'est-à-dire que les trames portent un identificateur du VLAN auquel elles appartiennent. Cette étiquette se résume par deux octets ajoutés dans la trame, selon les recommandations du comité 802 (standard 802.1Q). Nous évoquerons plus loin ce standard et ses évolutions.

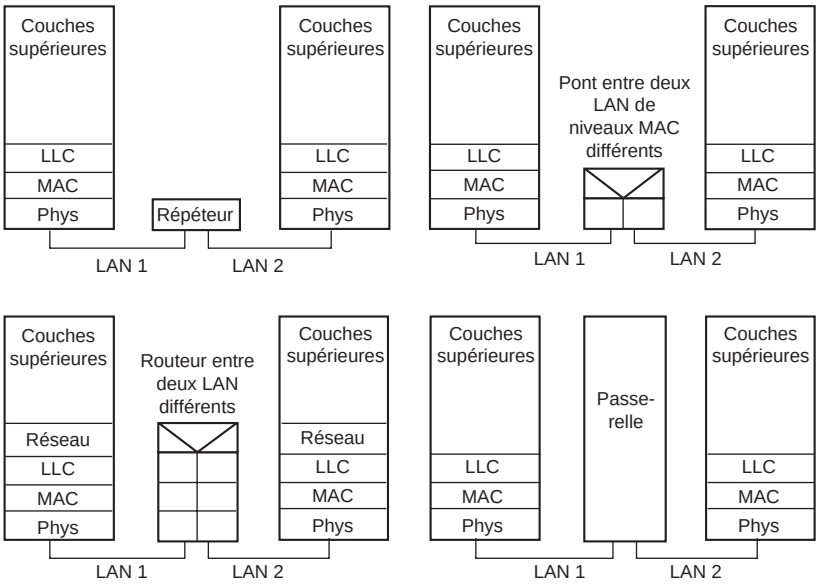
6 Interconnexion des réseaux locaux

Physiquement, deux réseaux ne peuvent être reliés que par l'intermédiaire d'un équipement connecté à chacun d'eux, sachant acheminer des messages de l'un à l'autre. Plusieurs dispositifs d'interconnexion se mettent en place, selon le degré de similitude des réseaux :

l'équipement d'interconnexion peut être selon les cas un *répéteur*, un *pont*, un *routeur* ou une *passerelle* (voir figure 5.14).

Figure 5.14

Répéteurs, ponts, routeurs et passerelles.



6.1 Répéteurs

Les *répéteurs* ne font que prolonger le support physique en amplifiant les signaux transmis. Ils propagent aussi les collisions. Ils sont utilisés pour relier deux segments de réseaux Ethernet, par exemple. Un répéteur n'a aucune fonction de conversion ou de transcodage. Il se contente de veiller à la répétition et à la régénération de signaux. Les répéteurs sont souvent utilisés pour s'affranchir des contraintes de distances préconisées dans les standards. Ils supposent donc que les architectures des sous-réseaux à relier soient identiques à partir de la couche MAC.

6.2 Ponts (*bridges*)

Les *ponts* (*bridges*) sont conçus pour construire un réseau local logique, à partir de plusieurs réseaux locaux, voisins ou distants. Ce sont des équipements qui interviennent au niveau de la couche LLC. Si les réseaux sont distants, deux demi-ponts peuvent être reliés par une liaison grande distance. Dans les deux cas, les réseaux reliés utilisent le même espace d'adressage MAC et constituent un réseau unique, les ponts étant transparents aux protocoles des couches supérieures. Les ponts améliorent les performances du réseau, dans la mesure où ils filtrent les collisions et ne les retransmettent pas. Ils ont évolué vers des équipements plus sophistiqués, comme les ponts *filtrants*, qui possèdent des fonctions particulières de sécurité et de contrôle du trafic : ils détectent, par exemple, les chemins redondants entre deux réseaux locaux grâce à un échange d'informations de gestion interne. L'algorithme exécute le protocole appelé STP (*Spanning Tree Protocol*), mis en œuvre pour éliminer le tronçon qui crée un chemin redondant et garder au réseau sa structure de bus ramifié.

Algorithme de l'arbre couvrant (*Spamming Tree*)

Cet algorithme, décrit dans le standard 802.1d[4], fait découvrir dynamiquement aux ponts un sous-ensemble sans boucle de la topologie du réseau. Pour cela, les ponts échangent des messages spéciaux permettant de calculer l'arbre couvrant. De tels messages sont

appelés *BPDU de configuration* (*Bridge Protocol Data Unit*). L'objectif des BPDU de configuration est de choisir :

- *Un pont unique de référence* (le pont *racine*). Ce pont sera considéré comme la racine de l'arbre parmi tous les ponts situés sur les réseaux locaux interconnectés.
- *Un pont dans chaque réseau local* (le pont *désigné*). Considéré comme le plus proche du pont racine, le pont désigné transmettra toutes les trames de ce réseau vers le pont racine.
- *Un port dans chaque pont* (le port *racine*). Ce port donne accès au meilleur trajet entre ce pont et le pont racine.
- *Les ports à inclure dans l'arbre couvrant*. Les ports qui composent l'arbre couvrant sont constitués du port racine, de tous les ports racine et de tous les ports où le pont est considéré comme pont désigné.

Le trafic des données est acheminé vers et en provenance des ports choisis pour faire partie de l'arbre couvrant. Jamais le pont ne retransmet de trames sur les ports n'en faisant pas partie : ces ports sont dans l'état bloqué.

Les BPDU sont transmises par un pont sur un port donné. Elles sont reçues par tous les ponts du réseau local rattaché au port et ne sont pas réexpédiées en dehors du réseau local. Dans une BPDU de configuration, l'adresse destination est une adresse spéciale attribuée à tous les ponts. L'adresse source est l'adresse physique associée au port : un pont possède autant d'adresses physiques que de ports. En outre, un pont possède un identificateur unique ID, codé sur 48 bits, qu'il utilise comme identificateur propre dans le champ de données d'un message de configuration. Nous utiliserons par la suite les termes :

- *ID racine*. Identification du pont supposé être la racine.
- *ID pont émetteur*. Identification du pont émettant le message de configuration.
- *Coût*. Coût du meilleur trajet depuis le pont émetteur jusqu'à la racine.
- *ID port*. Adresse physique d'un port.

À l'initialisation du protocole, chaque pont suppose qu'il est racine. Il émet donc des BPDU de configuration sur chaque port, avec son propre identificateur comme ID racine et ID pont émetteur et un coût nul vers la racine. Ensuite, il va recevoir continuellement des BPDU de configuration sur chaque port. Pour chacun d'eux, il sauvegarde le « meilleur » message de configuration, c'est-à-dire celui dont l'ID racine est le plus petit. En cas d'égalité d'ID racine, il choisit la BPDU dont le coût est le plus faible puis, si nécessaire, celle dont l'ID pont émetteur est le plus petit. Lorsque l'ID racine, le coût et l'ID pont émetteur sont identiques, c'est l'ID port qui sert d'arbitre. Une fois calculés la racine et le coût à la racine et après détermination du pont désigné sur chaque port, il faut décider quels ports doivent faire partie de l'arbre couvrant. Celui-ci est constitué du pont racine, de tous les ponts désignés et de tous les ports racine.

Exemple

Soit un pont d'ID = `92` qui a reçu un ensemble de BPDU de configuration conformément au tableau ci-après :

	ID racine	Coût	ID pont émetteur
Port 1	11	90	50
Port 2	11	83	41
Port 3	81	0	81
Port 4	17	32	26

4. Une version plus récente de cet algorithme est RSTP (*Rapid Spanning Tree Protocol*), décrit dans le standard 802.1w. Ce dernier protocole converge en quelques secondes au lieu d'une minute environ.

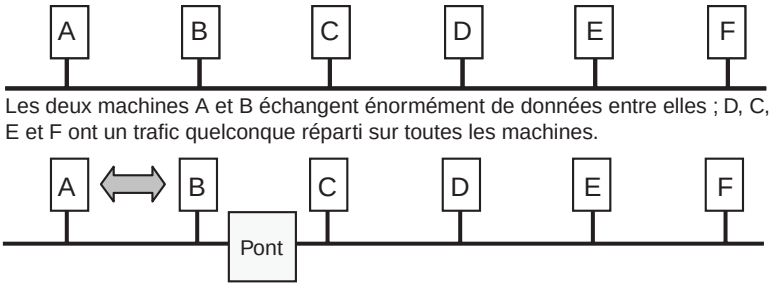
L'ID racine le plus petit est `11` ; le coût le plus faible parmi les messages ayant `11` comme ID racine est `83`, donc le port `2` est le port racine. Le pont détermine ensuite sa distance au pont racine en comptant `83 + 1` soit `84` (dans la réalité, le nombre 1 est le résultat d'une mesure). La BPDU de configuration que peut émettre notre pont vaut : `11.84.92`. Ce message est meilleur que celui qu'il a reçu sur les ports 1, 3 et 4. Le pont `92` est en conséquence pont désigné sur ces trois ports, sur lesquels il envoie sa BPDU de configuration.

Segmentation d'un réseau local

Les ponts permettent également de segmenter un réseau local en deux pour améliorer les performances. Par exemple, dans un réseau Ethernet qui approche de la saturation, on peut chercher les couples de machines qui ont un gros trafic entre elles et les isoler (voir figure 5.15). Le pont travaille par apprentissage : il apprend à situer les équipements progressivement, au fur et à mesure de leur activité. Dès qu'une trame se présente sur le pont et qu'elle est destinée au sous-réseau d'où elle vient, le pont la filtre (il ne la transmet pas dans un autre sous-réseau).

Figure 5.15

Segmentation d'un réseau local.



Un pont peut relier des réseaux locaux qui diffèrent par leur technique d'accès au support (un réseau utilisant CSMA avec un réseau utilisant des jetons, par exemple). Il doit alors gérer les différences de débit, de format, de méthodes d'accès et de services rendus. Le pont peut perdre des messages s'il est soumis pendant trop longtemps à des rafales de trafic sur l'un des réseaux qui dépassent la capacité de transmission sur l'autre. De plus, l'ensemble des différences nécessite un traitement dans le pont qui provoque un retard dans la transmission.

Grâce aux progrès technologiques, de nouveaux équipements, les commutateurs (*switches*), ont remplacé les ponts dans la plupart des installations. Ils prennent une place de plus en plus importante dans les réseaux d'entreprise car ils ont évolué et assurent désormais des fonctions plus sophistiquées que la simple commutation de trames.

6.3 Évolution des ponts : les commutateurs

L'essor des commutateurs a commencé à l'avènement des VLAN (que nous avons vu à la section 5.2). Le commutateur d'un réseau local peut être assimilé à un pont évolué à très hautes performances, qui transmet et filtre les trames grâce à ses tables de réacheminement. Dans les réseaux d'entreprise comptant plusieurs VLAN, les *trunks* sont des liaisons dédiées entre commutateurs, sur lesquelles circulent les données des différents VLAN.

Pour tenir compte des nouvelles topologies et des contraintes qu'elles ont imposées dans la circulation des flux d'information entre VLAN, certains protocoles antiboucles, comme

STP, ont été modifiés pendant que d'autres ont émergé : RSTP (*Rapid Spanning Tree*) ou 802.1w est la version modifiée de l'arbre couvrant qui permet une convergence plus rapide ; le MSTP (*Multiple Spanning Tree*), décrit dans le standard IEEE 802.1Q, permet de créer des arbres couvrants multiples pour les différents VLAN.

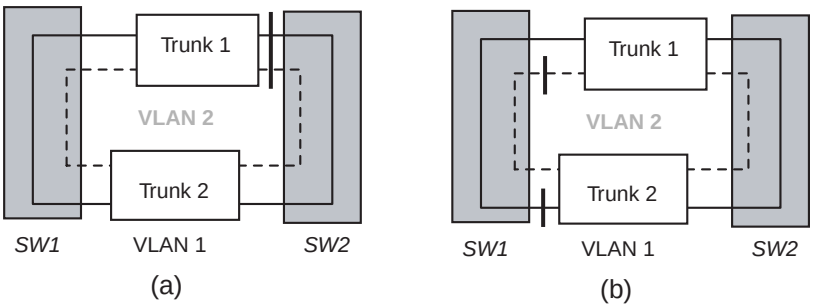
Arbre couvrant multiple dans les VLAN (802.1Q)

L'idée sous-jacente au concept de STP multiple est de proposer un algorithme qui tienne compte de la complexité de la circulation des flux des différents VLAN dans les trunks. Dans l'exemple de la figure 5.16a, deux commutateurs reliés par deux trunks transportent les données de deux VLAN (l'un des deux VLAN est en trait plein, l'autre en pointillé). La mise en œuvre d'un seul arbre couvrant conduit à bloquer un port dans chaque commutateur pour éviter les boucles. La figure 5.16b montre que l'utilisation de deux arbres couvrants évite ce problème.

Pour permettre une configuration dynamique des différents VLAN, les trunks doivent transporter les données de tous les VLAN.

Figure 5.16

Exemple de deux commutateurs reliés par deux trunks pour véhiculer les données de deux VLAN.



Configuration avec deux VLAN véhiculés sur deux trunks distincts entre les commutateurs SW1 et SW2. Un gros trait signifie qu'un port est bloqué.

(a) : Configuration utilisant un seul arbre couvrant. Pour éviter la création d'une boucle entre *SW1* et *SW2*, on ne peut pas se servir d'un des deux liens pour écouler le trafic normal des *VLAN*. Ici, *SW2* a ses deux ports bloqués : le second lien sert uniquement de secours en cas de panne du premier.

(b) : Configuration utilisant deux arbres couvrants. Dans ce cas, un des *trunks* transporte les données d'un *VLAN*, tandis que l'autre véhicule les données de l'autre *VLAN*. En cas de panne d'un *trunk*, le lien survivant peut transporter les données des deux *VLAN*.

Nous voyons bien que la contrepartie de la multiplication des VLAN dans le réseau de l'entreprise est la multiplication du nombre d'arbres couvrants à maintenir. Cette prolifération risque d'entraîner une gestion complexe de l'algorithme et provoquer une baisse des performances des commutateurs.

Pour rendre la circulation entre VLAN plus efficace, il s'est développé des techniques de *routage interVLAN*, naturellement assumées par les commutateurs, qui sont ainsi devenus des *commutateurs-routeurs*.

Commutateurs-routeurs

Les fonctionnalités de plus en plus étendues des commutateurs empiètent sur les fonctions classiquement dévolues aux routeurs. De ce fait, les commutateurs les plus sophistiqués sont souvent appelés des *commutateurs-routeurs*. Désormais, en plus des fonctions traditionnelles de commutation d'un port à l'autre, les commutateurs-routeurs sont capables d'effectuer des fonctions de niveau 3 et même de niveau 4 du modèle OSI.

Les fonctions de niveau 3 que peuvent exécuter les commutateurs-routeurs sont :

- Le routage interVLAN, en fonction des adresses IP.
- Le routage dynamique car ils peuvent exécuter les protocoles de routage comme RIP, OSPF, BGP… que nous verrons au chapitre 8.
- Le protocole VRRP (*Virtual Router Redundancy Protocol*), décrit par la RFC 2338. Ce protocole, de plus en plus utilisé – aussi bien dans les routeurs que dans les commutateurs-routeurs –, s'attache à résoudre le problème de l'unicité du routeur par défaut. Il est développé à la section suivante.
- La gestion de *listes de contrôle d'accès* ou ACL (*Access Control List*). Pour chaque sous-réseau IP, le commutateur peut autoriser ou interdire l'accès à tel autre sous-réseau IP, comme le fait normalement un routeur.

En plus des fonctions de niveau 3, les commutateurs-routeurs – comme la plupart des routeurs – peuvent inspecter le contenu des datagrammes IP. En effet, on peut affiner l'utilisation des listes de contrôle d'accès en autorisant ou en interdisant la circulation des flux de données sur certains ports TCP ou UDP. De la sorte, le commutateur-routeur se comporte comme un pare-feu de base décrit dans les compléments pédagogiques, sur le site www.pearsoneducation.fr.

Remarque

Ces nouvelles fonctions expliquent que les commutateurs sont des équipements d'interconnexion de plus en plus utilisés. Néanmoins, elles sont assurées en consommant des ressources (mémoire, processeur) utiles aux tâches normalement exécutées par les commutateurs : exécution du spanning tree et des autres protocoles antiboucles, apprentissage de la localisation des stations, gestion de la diffusion de niveau MAC, etc. En cas de trafic important, les performances du commutateur se dégradent si un grand nombre de listes de contrôle d'accès est mis en place.

Protocole VRRP (*Virtual Router Redundancy Protocol*) [RFC 2338]

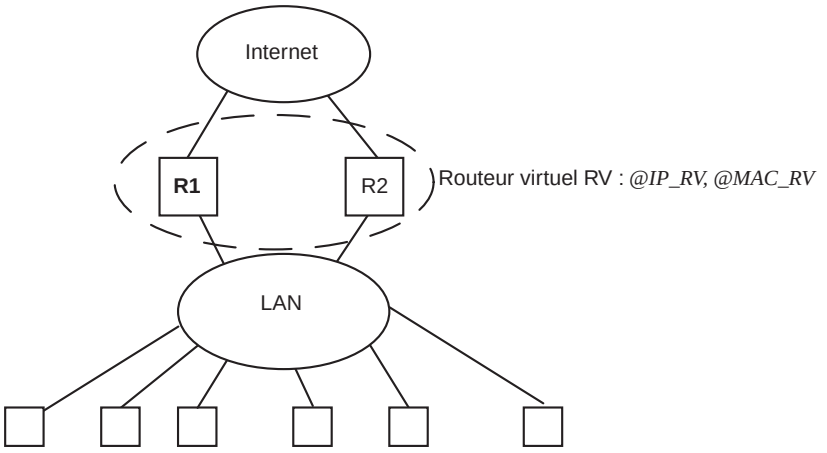
Le protocole VRRP est un standard Internet qui propose une solution permettant à un réseau de ne pas être complètement isolé lorsqu'un équipement d'interconnexion de niveau 3 (routeur ou commutateur-routeur), unique dans le réseau, tombe en panne. Par exemple, si le routeur de sortie du réseau de l'entreprise existant en un seul exemplaire ne fonctionne plus, le réseau est complètement isolé du monde extérieur. VRRP décrit comment installer plusieurs équipements de secours qui prennent, automatiquement et en très peu de temps, la relève de l'équipement défaillant. Pour cela, deux routeurs (ou plus[5]) se partagent une adresse IP et une adresse MAC virtuelles ; un seul routeur est actif (*Master router*) à l'instant *t*. En cas de panne du routeur actif, le changement de routeur est transparent pour les utilisateurs.

Les routeurs utilisant VRRP (les routeurs VRRP) se trouvent dans l'un des trois états suivants : *Initialize*, *Master* ou *Backup*. Dans l'état Initialize, le routeur attend un événement qui le fera basculer dans l'un des deux autres états. L'état Backup sert à vérifier que le routeur actif est bien dans l'état Master et qu'il est en fonctionnement. Dans l'état Master, le routeur actif informe les routeurs de secours (*Backup routers*) à intervalles réguliers qu'il peut toujours assurer le routage vers l'extérieur du réseau. La figure 5.17 donne un exemple d'utilisation de VRRP.

5. VRRP prévoit jusqu'à 255 équipements de secours mais la plupart des installations se contentent d'un seul équipement redondant.

Figure 5.17

Exemple de réseau utilisant le protocole VRRP.



R1 et *R2* forment le routeur virtuel. Ils possèdent leurs propres adresses *IP* et *MAC*. **R1** est le routeur actif. Les adresses réelles (*IP* et *MAC*) des routeurs sont respectivement : @IP_R1 ; @MAC_R1 pour le routeur R1 et @IP_R2 ; @MAC_R2 pour le routeur R2. Les machines du réseau ont comme seule adresse de routeur par défaut l'adresse du routeur virtuel, soit @IP_RV.

Les routeurs VRRP utilisent l'adresse MAC virtuelle : `00 00 5E 00 01 Id` du routeur VRRP (cet identifiant est codé sur un octet[6]). L'adresse IP virtuelle et les adresses IP réelles des routeurs sont déterminées par l'administrateur, en fonction de la structure du réseau.

Remarque

Il existe des variantes non standard de cet algorithme. On peut notamment citer le protocole HSRP (RFC 2281) de Cisco Systems Inc.

6.4 Routeurs (*routers*) et passerelles (*gateways*)

Les *routeurs* (*routers*) sont destinés à relier plusieurs réseaux de technologies différentes. Ils opèrent essentiellement au niveau de la couche 3 du modèle OSI, c'est-à-dire qu'ils assurent le routage des informations à travers l'ensemble des réseaux interconnectés. Le routeur possède au moins deux interfaces réseau et contient un logiciel très évolué, administrable à distance. Pour tenir compte de l'évolution des commutateurs, les routeurs proposent à leur tour des fonctions de niveau plus élevé que le niveau 3 : fonctions de pare-feu et autres, comme nous l'avons vu pour les commutateurs-routeurs. Ils sont liés à l'architecture des protocoles de routage utilisés, contrairement aux commutateurs. La majorité des routeurs utilisant le protocole IP, nous étudierons plus en détail leur fonctionnement au chapitre 6.

Enfin, les *passerelles* (*gateways*) sont des équipements qui relient des réseaux totalement différents : elles assurent une compatibilité au niveau des protocoles de couches hautes entre réseaux hétérogènes et effectuent, par exemple, des conversions vers des protocoles et des applications « propriétaires ». Notons que dans le jargon franglais des administrateurs de réseaux, le terme gateway désigne un routeur.

6. Les routeurs VRRP communiquent en multicast avec l'adresse `224.0.0.18`.

Remarque

Après avoir constaté l'évolution des commutateurs, on peut se demander dans ces conditions ce qui distingue réellement un commutateur-routeur d'un routeur…
Les routeurs ne se chargent pas de la gestion des VLAN (qui reste l'apanage des commutateurs), alors que les commutateurs ne gèrent pas de réseaux privés virtuels (VPN, *Virtual Private Network*[7]), pour lesquels les routeurs restent indispensables. En outre, le nombre de ports d'un commutateur est souvent beaucoup plus élevé que celui d'un routeur. Enfin, pour des fonctions de routage complexes, le routeur offrira de meilleures performances qu'un commutateur-routeur.

7 Réseaux locaux sans fil

Pour qu'une technologie puisse émerger, elle doit offrir, outre de nouvelles fonctionnalités, une certaine compatibilité avec des normes ou standards existants. Les contraintes qui ont guidé les concepteurs dans leurs choix techniques pour concevoir des réseaux sans fil étaient nombreuses : trouver une bande de fréquences disponible (de préférence mondiale) pour une grande diffusion des produits, tenir compte de la portée limitée des signaux radio, préserver la confidentialité des communications et de la durée de vie limitée des batteries des stations nomades, disposer d'une bande passante suffisante pour que le système soit viable économiquement et assurer une compatibilité ascendante. Le standard 802.11 pour réseaux locaux sans fil (WLAN, *Wireless LAN*) a été conçu pour être compatible avec Ethernet. De ce fait, les protocoles situés au-dessus de la couche MAC sont utilisés sans aucune modification.

Dans un WLAN, l'écoute préalable du signal avant émission ne fonctionne pas très bien, pour plusieurs raisons : par exemple, la disparité des puissances d'émission des différentes stations et la réflexion des ondes radio par des objets solides, entraînent des réceptions multiples du même message.

Après une brève description des standards de réseaux sans fil, nous présentons les techniques de transmission spécifiques de ces réseaux avant d'évoquer les différentes architectures : les réseaux *ad hoc* et les réseaux *à infrastructure*.

7.1 Standards des réseaux sans fil

On distingue deux grandes catégories de réseaux sans fil, selon leur usage et les performances attendues (voir tableaux 5.1 et 5.2) :

- réseaux sans fil (WLAN) compatibles Ethernet, standardisés par 802.11 ;
- réseaux sans fil (WPAN, *Wireless Personal Area Network*), reliant des assistants personnels (PDA), téléphones, etc. Standardisés par 802.15, ils sont plus connus sous le nom de Bluetooth.

Tableau 5.1

Normes WLAN

Normes WLAN	Nom commercial	Débit théorique en Mbit/s	Portée max
ETSI 300 652	Hiperlan1	20	–
ETSI (en cours)	Hiperlan2	54	30 m
802.11a	Wi-Fi	54	40 m
802.11b	Wi-Fi	11	90 m
802.11g	Wi-Fi	54	70 m
HomeRF 1.0	HomeRF	1,6	50 m

7. Les VPN sont présentés dans les compléments pédagogiques, sur le site www.pearsoneducation.fr.

Tableau 5.2
Normes WPAN

Normes WPAN	Nom commercial	Débit théorique en Mbit/s	Portée max
IrDA	FIR (Fast IR)	4	1 m
802.15.1	Bluetooth	1	30 m
802.15.3	Bluetooth 2	12	10 m
802.15.4	Zigbee	0,250	75 m

7.2 Techniques de transmission utilisées dans le standard 802.11

La bande de fréquences la plus utilisée pour les réseaux sans fil est dans la bande 2,4 GHz [2,4-2,4835 GHz]. Celle-ci est partagée par d'autres domaines d'applications (four à micro-ondes, transmetteurs domestiques, relais, télémesures, télémédecine, caméras sans fil…). Il y a donc des risques d'interférences ! Pour transmettre les données, les réseaux sans fil utilisent des combinaisons de modulations adaptées aux transmissions par radio (variantes de modulation de fréquence ou de phase) mais aussi des techniques spécifiques comme les techniques à étalement de spectre (*spread spectrum*) : elles utilisent une bande de fréquences large pour transmettre des données avec une faible puissance d'émission. La technique consiste à découper la large bande de fréquences en au moins 75 canaux de 1 MHz : dans la bande des 2,4 GHz, on peut ainsi créer 79 canaux de 1 MHz. La transmission s'effectue pendant environ 400 ms sur un canal puis sur un autre, en utilisant une combinaison de canaux connue de toutes les stations de la cellule.

Dans le standard 802.11b, la bande de 2,4 GHz est découpée en 14 canaux séparés de 5 MHz. Aux USA, seuls les 11 premiers canaux sont utilisables. En France, on n'utilise que les canaux 10 à 13. Pour transmettre correctement à 11 Mbit/s, il faut une largeur de bande de 22 MHz (théorème de Shannon). De ce fait, certains canaux recouvrent partiellement des canaux adjacents : il faut choisir des canaux isolés les uns des autres (par exemple, les canaux 1, 6 et 11). Dans la pratique, on utilise généralement des canaux distants de 25 MHz les uns des autres. Il faut donc organiser les points d'accès et l'utilisation des canaux pour éviter les interférences.

Dans le standard 802.11a, on utilise la bande des 5 GHz [5,15-5,35 GHz] et [5,725-5,825 GHz] et 8 canaux distincts, chacun ayant une largeur de 20 MHz.

7.3 Architectures des réseaux sans fil

Deux modèles d'architecture sont à considérer : les *réseaux ad hoc* et les *réseaux à infrastructure*. Dans les réseaux *ad hoc*, les communications s'effectuent en point à point entre les stations. C'est le modèle de fonctionnement des WPAN. Dans les réseaux à infrastructure, le réseau est géré par une ou plusieurs *bases* (ou *bornes* ou *points d'accès*). Lorsqu'un réseau comprend plusieurs bornes, celles-ci sont raccordées par un réseau Ethernet filaire. Chaque borne offre un ensemble de services appelés BSS (*Basic Service Set*). Les bases servent de ponts entre le réseau filaire et le réseau sans fil. Lorsqu'il existe plusieurs bornes, il faut mettre en place un service étendu afin de permettre aux utilisateurs de se déplacer d'une base à l'autre. L'ensemble des bornes constitue le *système de distribution*. Outre l'acheminement des données, les services fournis par un système de distribution sont :

- *L'authentification* (pour ajouter une station dans le réseau). Elle se fait le plus souvent par l'adresse MAC. La *désauthentification* est le service opposé au précédent qui gère correctement la sortie d'une station du WLAN.

- *L'association*. Elle permet à une station d'échanger des données *via* un point d'accès auprès duquel elle s'est identifiée. La *réassociation* permet d'aller d'une base à l'autre tandis que la *désassociation* permet de quitter une base ou le WLAN.
- La *confidentialité*. Cela consiste à utiliser une méthode de chiffrement.
- La *distribution*. C'est l'équivalent du routage dans un réseau classique.

7.4 Méthode d'accès dans les WLAN

802.11 utilise CSMA/CA (*Collision Avoidance*) pour gérer les contentions d'accès à la fréquence partagée par toutes les stations d'une base. Une station n'émet que si elle ne détecte pas de trafic sur la bande de fréquences partagée. Sinon, elle attend un temps aléatoire avant de se remettre à l'écoute. Pour minimiser les collisions, on utilise souvent un mécanisme optionnel : avant de lui envoyer une trame, la base envoie d'abord à la station une trame RTS (*Request To Send*), à laquelle celle-ci doit répondre et attendre ensuite la réception de la trame de données. Les autres stations, qui détectent la trame RTS, retardent leur éventuelle émission.

Contrairement à Ethernet, les récepteurs doivent envoyer une trame d'acquittement (ACK) pour chaque trame d'informations reçue, car les fréquences radio peuvent être perturbées. De plus, pour minimiser l'impact des interférences, les stations échangent des trames courtes.

Les stations doivent pouvoir passer d'une base à l'autre sans que la communication soit coupée (*roaming*). La station, identifiée auprès de plusieurs bases, détermine la meilleure (celle qui lui offre la meilleure qualité de transmission), avec laquelle elle doit être en contact, et se réassocie avec.

Remarque

Le nom BSS est parfois synonyme de borne dans la terminologie des réseaux sans fil.

Résumé

L'utilisation d'un support unique partagé entre plusieurs utilisateurs d'un réseau local nécessite la mise en œuvre de méthodes d'accès spécifiques (accès aléatoire avec détection de porteuse ou mécanismes à jetons). Par ailleurs, les réseaux locaux permettent la diffusion de l'information dans tout le réseau. Grâce à sa simplicité et sa capacité d'adaptation, Ethernet est le réseau le plus répandu. Depuis les origines, il a su évoluer du réseau en bus à 10 Mbit/s jusqu'au réseau en étoile autour d'un commutateur pouvant gérer des réseaux locaux virtuels avec des débits dépassant le Gbit/s. Selon le niveau de l'interconnexion, les réseaux locaux se relient au monde extérieur par différents équipements : répéteurs, ponts, commutateurs, commutateurs-routeurs, routeurs et passerelles. En outre, nous avons présenté les particularités des réseaux locaux sans fil.