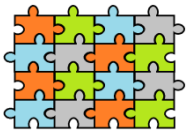


Réseaux de télécommunication

Caractéristiques des réseaux

Un réseau informatique consiste en la connexion de plusieurs ordinateurs de manière à ce qu'ils puissent échanger des messages et des données. Un ordinateur connecté à un réseau est souvent appelé **hôte**. Il se connecte usuellement à partir d'une carte spéciale : la carte réseau.

Un certain nombre de conditions doit être réuni pour que le réseau fonctionne :

- les ordianteurs doivent respecter des règles d'émission et de réception appelées **protocoles**.
- les ordinateurs doivent pouvoir être identifiés sans ambiguité sur un réseau : par une **adresse unique** (à l'image du courrier postal : un destinataire doir posséder une adresse clairement définie).
- le réseau doit acheminer les messages et les données dans un **délai raisonnable et sans erreurs**. Or les transferts se font par envoi et réception de "0" et de "1" et il très courant, par suite d'une erreur d'origine électromagnétique ou suite à un parasitage, qu'un symbole binaire soit remplacé par un autre (un "0" par un "1" par exemple).

Les avantages d'un réseau ne sont plus à mettre en avant pour convaincre. Aujourd'hui, dans notre société de l'information, tout le monde est convaincu de l'utilité des réseaux. Citons cependant quelques avantages courants :

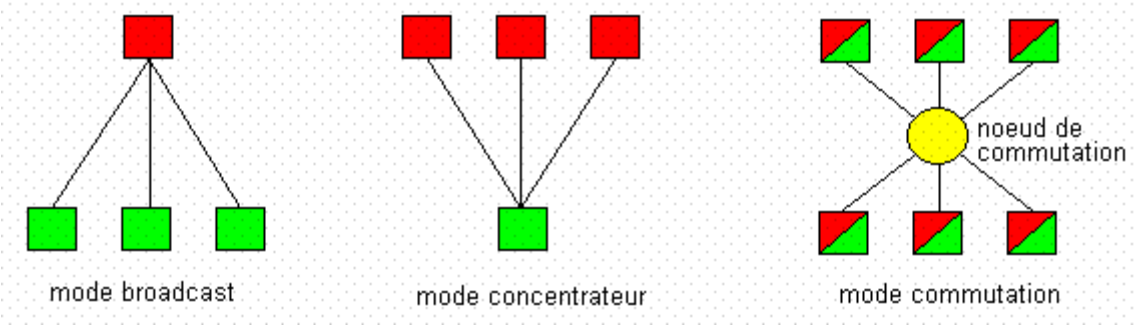
- un réseau permet la communication pour le travail ou le plaisir
- un réseau permet la répartition du travail ou le travail à distance
- un réseau permet de partager des données (bases de données communes) ou des services (en particulier l'accès à des périphériques mutualisés comme une imprimante couleur de haute qualité) ; les ordinateurs proposent des ressources ou des services sont appelés serveurs. On peut distinguer des serveurs de ressources, des serveurs Web (accessibles via un navigateur), des serveurs de données, des serveurs d'archivage, des serveurs d'impression, etc.

On peut classer les réseaux suivant plusieurs critères :

- critère fonctionnel : dispositif permettant d erelier des "communicants"
- critère géographique : LAN, MAN, WAN
- critère de service : fourniture de services liés au transport de données avec ou sans valeur ajoutée
- critère organisationnel : structure de travail indépendante de la distance (et éventuellement du temps)

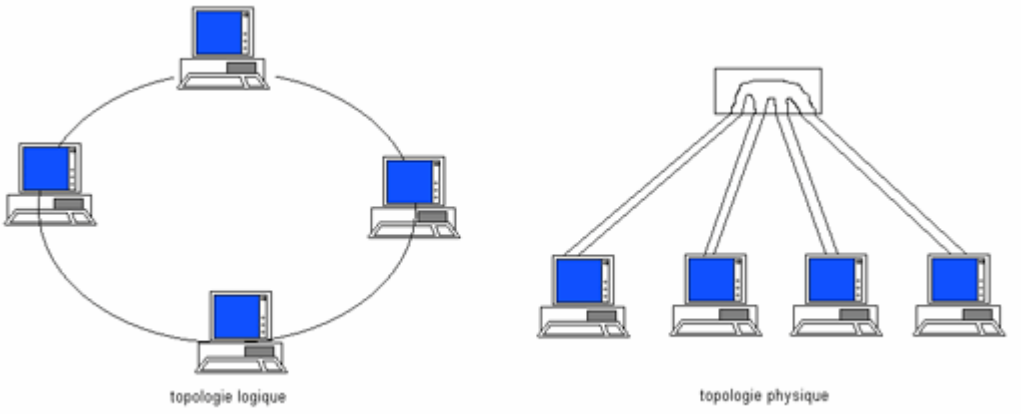
Le mode de diffusion des données sur un réseau permet de distinguer

- le mode **broadcast** : diffusion (1:N) d'un hôte vers tous les autres ; un cas particulier est le mode **multicast** : diffusion d'un hôte vers un groupe particulier d'hôtes (par exemple un sous-réseau).
- le mode **concentration** : diffusion (N:1) de tous les hôtes vers un seul
- le mode **commutation** : établissement de relations 1 à 1. Ce mode permet évidemment de recouvrir les précédents.

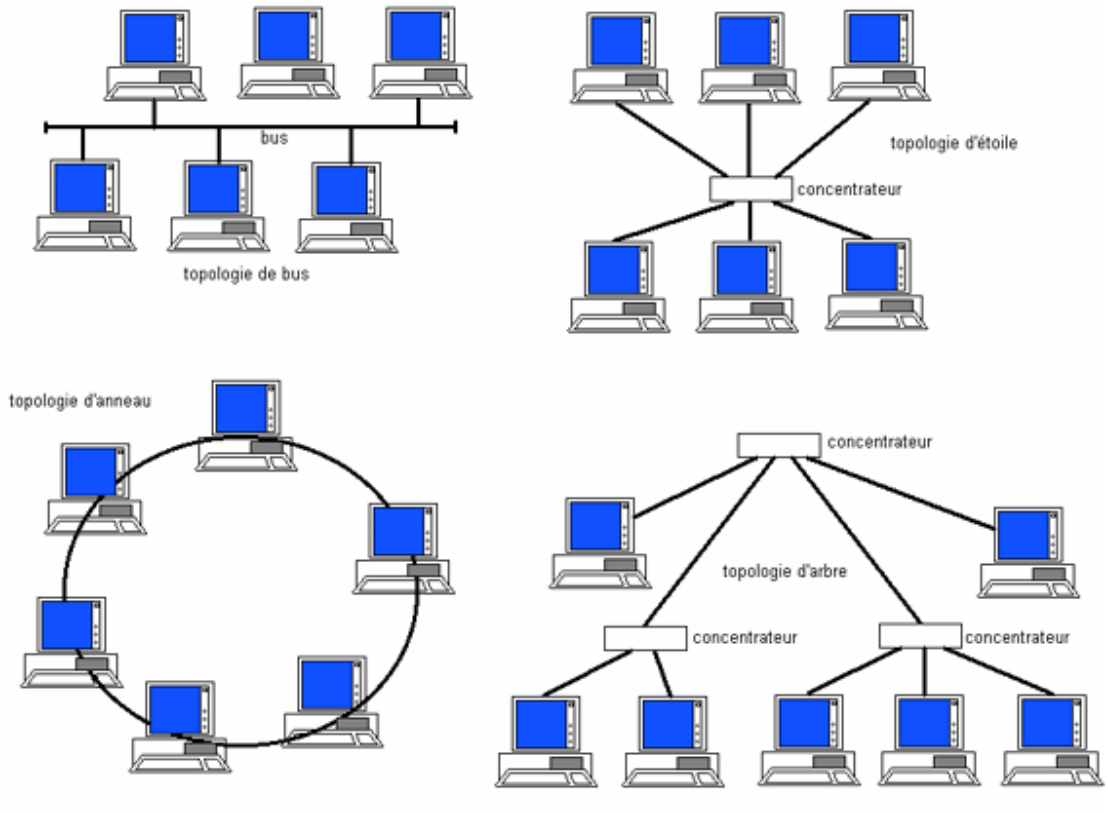


La commutation est universellement utilisée pour relier des hôtes dans un réseau étendu. Celui-ci utilise alors des hôtes spéciaux appelés **commutateurs**.

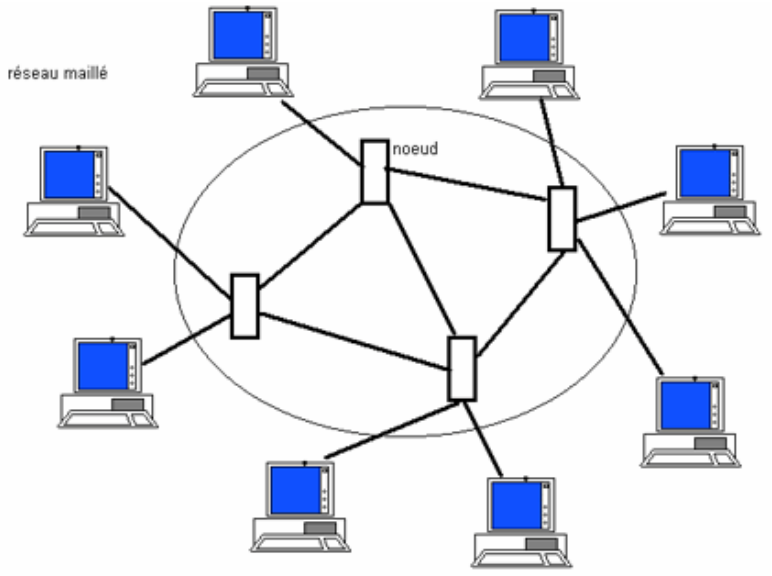
Une notion importante en matière de réseaux est la **topologie**, c'est à dire la manière dont les hôtes sont reliés entre eux au travers d'un réseau. Il faut distinguer à ce sujet la topologie logique et la topologie physique. Une topologie logique en anneau peut apparaître comme une topologie physique en étoile :



Les principales topologies sont résumées dans le schéma ci-dessous :



Un réseau important comme un réseau longue distance possédera une topologie plus complexe ; c'est le cas des réseaux maillés :



Suivant le critère géographique on distingue les réseaux locaux (LAN) , les réseaux métropolitains (MAN) et les réseaux longue distance (WAN).

Les réseaux locaux

Ce sont les réseaux élémentaires, ne comportant que peu d'ordinateurs connectés et d'extension géographique faible (moins de 1 km ; implantation dans un bâtiment par exemple). On les appelle LAN (Local Area Network).

les réseaux métropolitains

Ils constituent usuellement une interconnexion de réseaux locaux au niveau d'une aire géographique correspondant par exemple à un campus universitaire ou une agglomération. Ils sont appelés MAN (Metropolitan Area Netwok).

les réseaux longue distance

Ils correspondent à des interconnexions, en général complexes, de réseaux locaux et d eréseaux métropolitains. Ils parcourent aujourd'hui la Terre entière, notamment grâce à Internet qui est un procédé d'interconnexion de réseaux existants. On les appelle WAN (Wide Area Network).

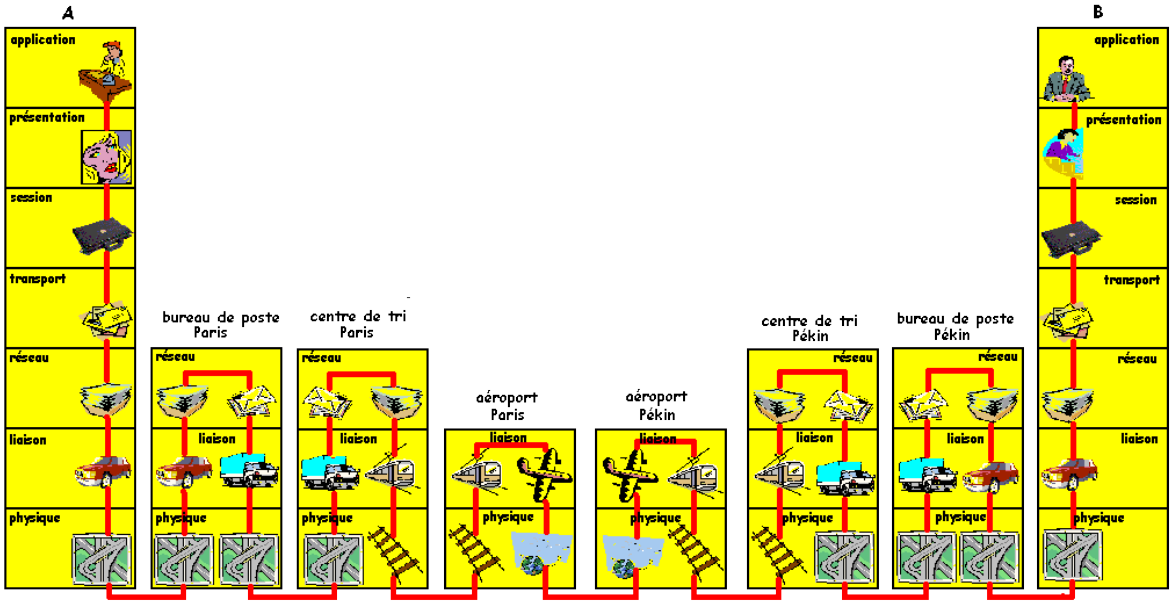
Modélisation et protocoles

Un réseau de transmission de données est souvent exprimé sous la forme d'un modèle en couches. Pour faire comprendre ce concept, imaginons une modélisation de la poste internationale. Deux correspondants A, à Paris, et B, à Pékin s'envoient du courrier postal. Comme A ne parle pas le chinois et que B ne parle pas le français, la langue anglaise, supposée compréhensible par un nombre suffisant de personnes, sera choisie pour correspondre. Admettons aussi que ces deux correspondants envoient leur courrier à partir de leur lieu de travail (entreprise par exemple) : leur courrier partira donc en même temps que le courrier de leur entreprise qui est géré par un service courrier.

Imaginons alors la succession d'événements pour que A envoie une lettre à B.

- A écrit la lettre en français avec son stylo.
- A donne sa lettre à une secrétaire anglophone qui la traduit en anglais, la met dans une enveloppe et écrit l'adresse de B
- La personne chargée du ramassage du courrier passe dans le service de A pour ramasser le courrier.
- Le service courrier effectue un tri du courrier et l'affranchit avec une machine à affranchir.
- Le courrier est déposé au bureau de poste.
- Le courrier est chargé dans une voiture qui l'emmène au centre de tri
- Le courrier pour la Chine est emmené à l'aéroport de Paris par train
- Le courrier pour la Chine est transmis par avion à l'aéroport de Pékin
- Le courrier est transmis par train de l'aéroport de Pékin au centre de tri de Pékin
- Le courrier pour l'entreprise de B est transmis à l'entreprise par voiture
- Le service courrier de l'entreprise de B trie le courrier arrivé par service
- Le courrier est distribué à heure fixe aux destinataires et en particulier au service de B
- La secrétaire de B ouvre le courrier et traduit en chinois le contenu de la lettre destinée à B
- B lit la lettre que lui a envoyée A.

On peut résumer par un schéma la succession des évènements afin de mettre en évidence un modèle en couches et les noeuds du réseau:



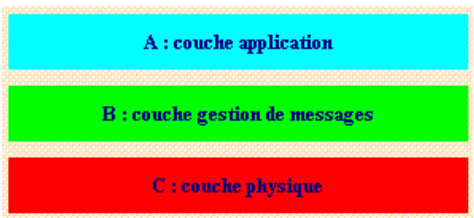
La dénomination des couches est conforme à un standard appelé OSI (Open System Interconnect) qui sera étudié plus loin. Sur cet exemple, à but uniquement pédagogique, basé sur un réseau postal (imaginaire !), explicitons les fonctionnalités de chaque couche.

- couche application : écriture/lecture de la lettre
- couche présentation : traduction, mise en forme, ouverture de lettre
- couche session : relevé/distribution du courrier dans les services
- couche transport : action du service courrier
- couche réseau : action du bureau de poste ou du centre de tri
- couche liaison : acheminement de la lettre entre deux noeuds consécutifs du réseau
- couche physique : utilisation des supports de communication

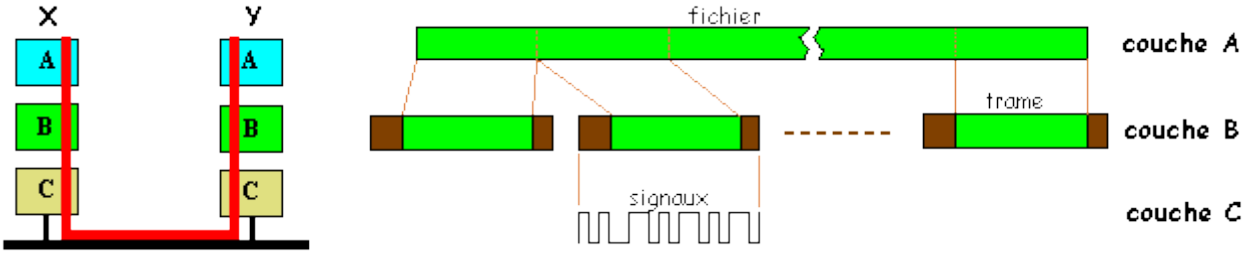
Dans cette modélisation, chaque couche est bâtie sur la couche inférieure. Par exemple, le transport routier (couche liaison) a besoin de l'infrastructure routière (couche physique).

Pour chacune des couches, des fonctionnalités (ici très résumées) sont définies qui sont des services rendus aux couches supérieures. Les lignes rouges du schéma indiquent la suite de services rendus par les différentes couches. Par ailleurs, les fonctionnalités de chaque couche correspondent à des règles appelées protocoles.

Prenons maintenant un exemple plus "télécommunications" en envisageant un transfert de fichier entre un ordinateur X et un ordinateur Y reliés par un câble série. On peut envisager une modélisation à 3 couches :



L'utilisateur désirant transférer un fichier fait appel à la couche A à l'aide d'une primitive du type envoyer_fichier (nom du fichier, destinataire).
La couche A découpe le fichier en messages et transmet chaque message à la couche B par une primitive du type envoyer_message (numéro de message, destinataire).
La couche B effectue la gestion de l'envoi de message, éventuellement en découpant le message en unités intermédiaires (trames) ; l'envoi des trames entre X et Y obéissent à des règles (protocole) : cadence d'envoi, contrôle de flux, attente d'un accusé de réception, contrôle de erreurs.
La couche B fournit à la couche C un train de bits qui sera acheminé, indépendamment de sa signification, via une voie de transmission physique, vers le destinataire.
L'information est transmise par une voie de communication plus ou moins complexe et chemine, au niveau du destinataire dans le sens inverse de ce qui vient d'être décrit: émetteur et récepteur possède des couches identiques.

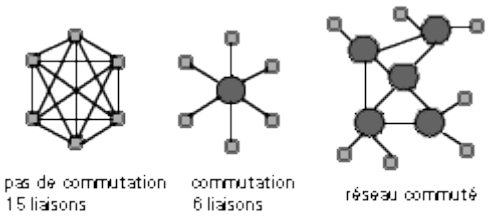


On notera aussi que les unités d'information diffèrent suivant les trois couches. Pour la couche A, l'unité est un fichier, c'est à dire une suite importante de bits. Pour la couche B, l'unité d'information est la trame qui possède une structure définie (information utile + information de service). Pour la couche C, l'unité d'information est le signal transmis sur le support physique de communication.

Commutation et multiplexage

Ce sont les deux technologies qui caractérisent les réseaux.

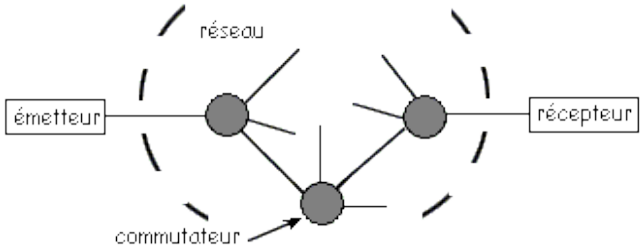
Pour la communication entre usagers, la commutation est essentielle. Il est en effet impensable de relier chaque usager à tous les autres. En effet, si l'on voulait relier n stations directement à chacune d'elles, il faudrait établir n(n-1)/2 liaisons ce qui est impensable au niveau planétaire.



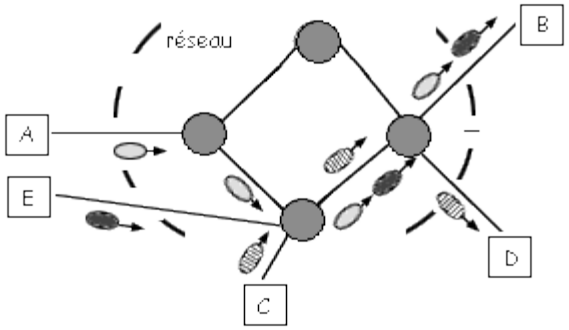
On est conduit logiquement à construire les réseaux à partir de **nœuds de commutation**. Ces nœuds de commutation sont chargés d'acheminer dans la bonne direction les informations qu'ils reçoivent. Cette fonctionnalité est appelée **routage**.

En fait, la commutation peut se concevoir de manières différentes

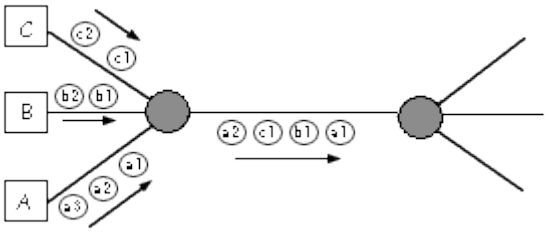
- commutation de circuits : elle consiste à réquisitionner, pour une communication, des tronçons de réseau pour assurer une liaison de bout en bout ; les tronçons sont liés les uns aux autres à chaque nœud de commutation ; la communication terminée, les tronçons sont libérés et disponibles pour une nouvelle commutation. Cette méthode est bien connue en téléphonie.



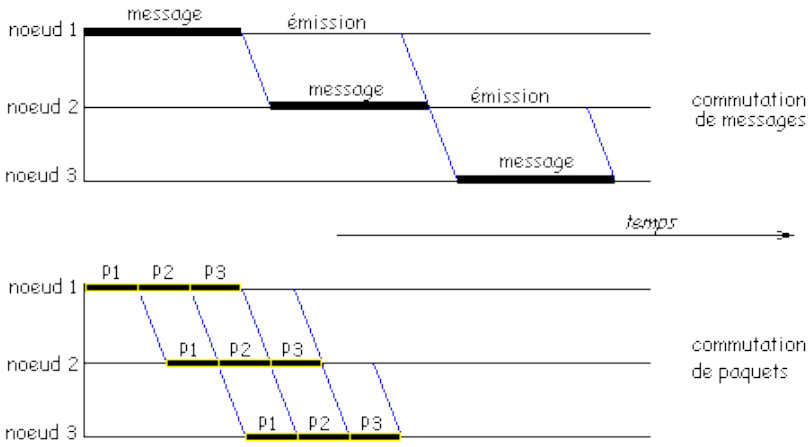
- commutation de messages : l'information à transmettre est découpée en messages ; les messages circulent sur le réseau à manière du transport automobile. Chaque nœud de commutation sert de routeur mais aussi d'hébergement des messages en situation d'engorgement des tronçons du réseau. Ce mode de commutation a pratiquement disparu au profit de la commutation de paquets.



- commutation de paquets : chaque message est découpé en paquets de petite taille qui sont numérotés pour un ré-assemblage éventuel. Les paquets circulent dans le réseau et les nœuds de commutation en effectuent le routage et l'hébergement. Sur un tronçon, les paquets se suivent, même s'ils n'appartiennent pas au même message.



L'intérêt de la commutation de paquets sur la commutation de messages peut être rendu évident par la figure ci-dessous ; on gagne du temps par la simultanéité de réception et de transfert de paquets différents. Il faut en effet qu'un nœud "assimile" un bloc de bits (message ou paquet) avant de l'envoyer au nœud suivant. Rappelons que le débit est principalement lié à la vitesse d'"assimilation" car ensuite la transmission s'effectue à la vitesse de la lumière.



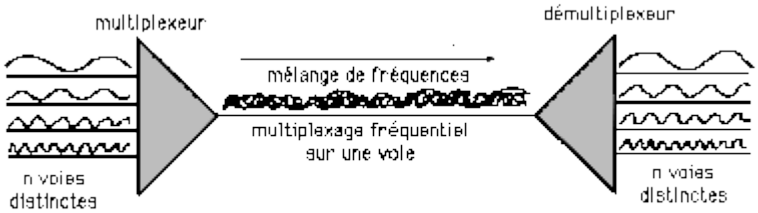
Il existe deux types de commutation de paquets

- le **circuit virtuel** : tous les paquets d'un même message suivent le même chemin défini pour chaque message ; la méthode est similaire à celle de la commutation de circuits.
- le **datagramme** : chaque paquet d'un message peut emprunter un chemin différent des autres ; à l'arrivée, il faut réordonner les paquets du message car des paquets peuvent aller plus vite que d'autres puisqu'empruntant des chemins différents.

Le multiplexage consiste à faire passer plusieurs messages sur un même tronçon de réseau ce qui permet une économie considérable. On distingue deux types de multiplexage :

- **multiplexage spatial**

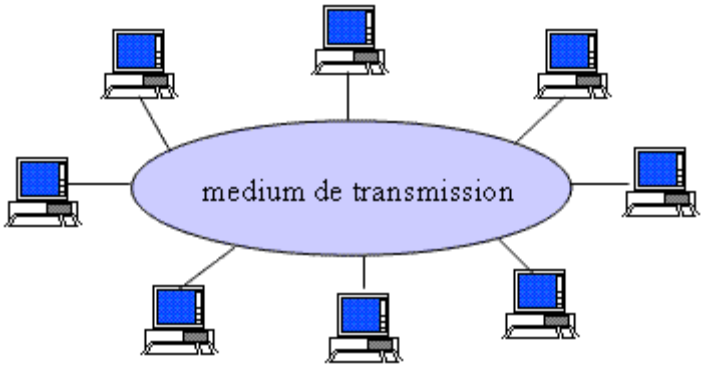
La bande passante du canal est divisée en sous-bandes (canaux) chaque message correspond à une sous-bande de fréquence ; un multiplexeur mélange les différents messages ; un démultiplexeur, à l'arrivée, sépare, grâce à un filtrage en fréquence, les messages.



- **multiplexage temporel** : ce type de multiplexage est bien adapté aux réseaux à commutation de paquets. Le multiplexeur n'est autre qu'un mélangeur de paquets, le démultiplexeur est un trieur de paquets.

Réseaux locaux

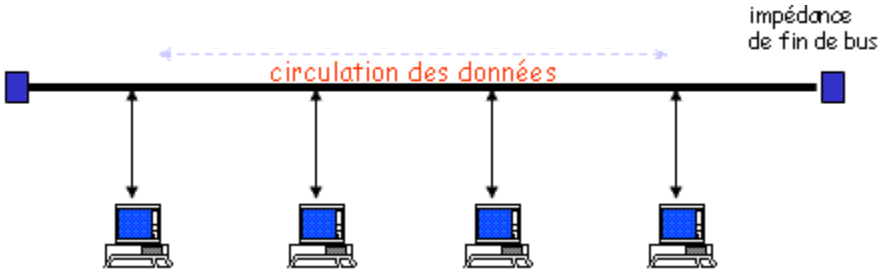
Dans un réseau local, les paquets d'information sont transmis vers un medium de transmission auquel sont rattachés les ordinateurs (appelés stations dans le cas de réseaux locaux) : donc quand une station émet, toutes les autres stations reçoivent théoriquement cette émission.



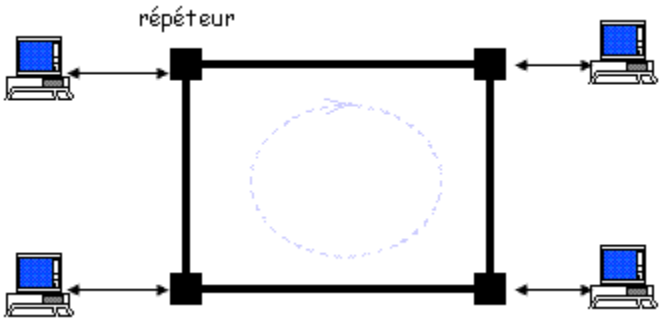
Les réseaux locaux diffèrent principalement par leurs protocoles et leurs topologies.

Les deux topologies logiques de base sont le bus et l'anneau.

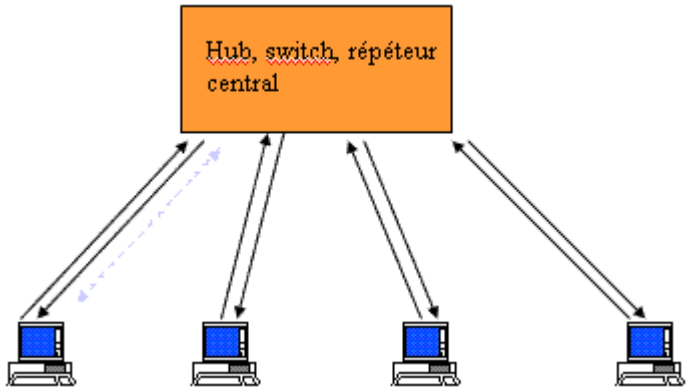
La topologie de bus (famille Ethernet) peut être représentée par un "câble" sur lequel se connectent les stations. Une émission donne lieu à un transport de bits dans les deux directions pour atteindre toutes les station :



La topologie d'anneau (famille Token Ring) est une boucle fermée sur laquelle se connectent les stations. La circulation de l'information s'effectue toujours dans le même sens :



Bien entendu, les topologies physiques peuvent être différentes. En général, elles sont, de nos jours, en étoile par l'intermédiaire de dispositifs de connexion ergonomiques ayant quelquefois des fonctions supplémentaires (répétition, concentration, commutation,...)



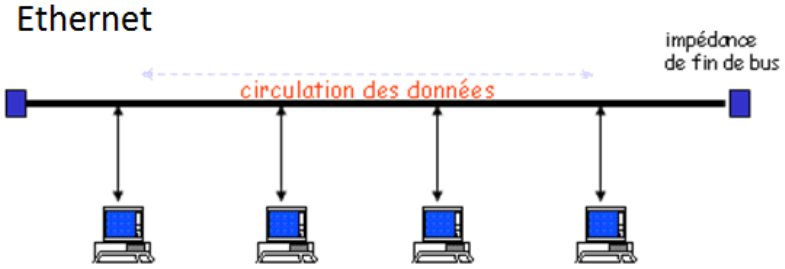
Standards de réseaux locaux

En ce qui concerne les standards de réseaux locaux, historiquement deux standards sont prépondérants : les réseaux de type Ethernet et les réseaux de type anneau à jeton. Ces standards concernent des réseaux filaires (paires torsadées, câble coaxial ou fibre optique). Donnons quelques caractéristiques rapides de ces standards.

Ethernet

Ce standard utilise un "bus" comme média de communication. Toutes les transmissions de données passent par ce bus unique mais on peut connecter un bus à un autre bus pour avoir un réseau plus étendu. Toutes les stations (postes client ou serveurs) sont connectées à ce bus. L'idée d'Ethernet (à ne pas confondre avec Internet) est simple et s'appuie sur deux directives protocolaires :

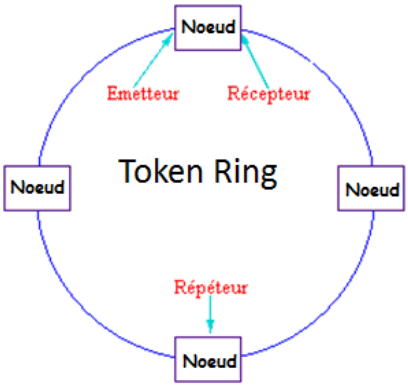
- CSMA (carrier Sense Multiple Access) : Avant d'émettre toute station se doit d'"écouter" s'il y a du bruit sur le bus. Si oui, alors une communication est en cours et il faut attendre le silence pour émettre. Cette directive est appelée "LST" (Listen Before Talk, ou écouter avant de parler, ce qui est une belle maxime applicable à toute conversation !)
- CSMA/CD où CD signifie Collision Detection, c'est à dire détection de collision. En effet, lorsque le bus est "silencieux", il peut arriver que deux stations émettent en même temps. Les signaux envoyés entrent alors en collision de cqui se manifeste par un bruit particulier très détectable. Comme les signaux émis par les stations se propagent dans les deux direction, chaque station émttrice verra revenir vers elle le bruit d'une collision. Elles doivent alors cesser d'émettre (car les informations seront incompréhensiles). Elles reprendront plus tard. Cette directive est appelée "LWT" (Listen While Talk ou écouter tout en parlant).



Token Ring

Pour l'anneau à jeton ou Token Ring, le principe est très différent. Tout d'abord, la structure topologique est en anneau sur lequel sont connectées les stations. Une trame tourne perpétuellement dans le même sens sur cet anneau avec un jeton (qui n'est autre qu'un bit) mis à 0 si la trame est libre et à 1 si elle est occupée.

Une station qui veut émettre attend le passage de la trame et lit le jeton. Si la trame est occupée, la station attend son prochain passage. Si la trame est libre, elle met le jeton à 1 et place dans la trame l'adresse de la station destinatrice et l'information à transmettre. La trame continue son chemin et au passage de chaque station (elle les rencontre toutes) la lecture de l'adresse destinataire permet de savoir si le message est à prendre ou à laisser. Lorsque qu'une station reconnait son adresse, elle s'approprie le message mais ne change pas le jeton. Quand la trame repassera devant la station émettrice (ce qui vaut un accusé de réception), le jeton sera remis à 0.



WIFI

Wi-Fi ou WiFi ou Wifi signifie Wireless Fidelity. Il s'agit d'un standard de réseau local sans fil obéissant à la norme 802.11b (et maintenant 802.11g qui est compatible avec la précédente). Il s'agit d'un réseau haut débit dont la couverture se veut "large" à l'instar de la téléphonie mobile et est prévu pour une connexion à Internet.

WiFi utilise la technique DS (Etalement de spectre par codage) pour éviter les brouillages.

WiFi utilise des cartes sur les stations dont le but est de se connecter sur un point fixe (borne). Le débit théorique est de 11 Mbits/s. La portée du réseau est liée à la puissance des bornes, en général de 30 m à 100 m. La plage de fréquences utilisée est celle des 2,4 GHz. En France, cette plage était exploitée par les militaires ; elle est maintenant libérée. Rappelons à ce sujet les caractéristiques de WiFi et de ses principaux concurrents :

technologie	plage de fréquences	débit théorique	portée max	usage
WiFi	2,4 GHz	11 Mbits/S	100 m	entreprise, métropole
HomeRF	2,4 GHz	1,6 Mbits/s	30 m	usage personnel
Bluetooth	2,4 GHZ	1 Mbits/s	10 m	usage personnel, mobilité
Hiperlan	5 GHz	54 Mbits/s	100 m	réseaux locaux

Contrairement à Bluetooth dont la portée est faible, WiFi du fait de plus grande portée pose le problème de la sécurité des transactions. Les failles sont de deux types :

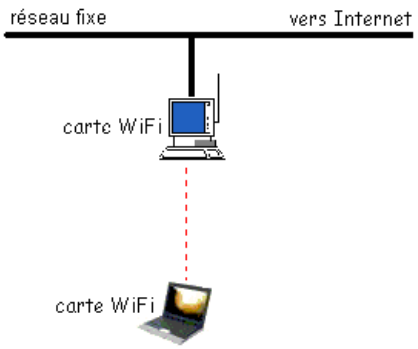
- l'écoute clandestine est facile car les émissions peuvent être captées par des stations non autorisées.
- WiFi utilise un protocole de sécurité WEP (Wired Equivalent Privacy) qui est largement critiqué

Le Monde Informatique : 14 février 2001

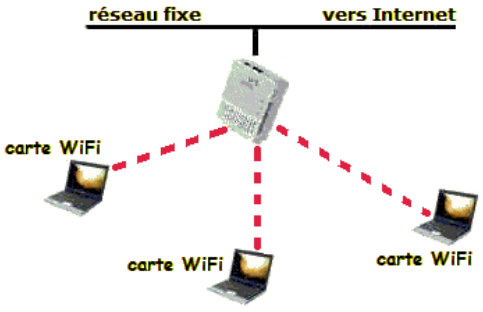
Les failles de sécurité des WLAN aux normes 802.11
« Les réseaux sans fil au standard 802.11 ne sont pas sûrs. […] Le protocole WEP pêche surtout par le fait qu'il n'assure pas la sécurisation de la distribution des clés d'encryptage. […] Seul 3Com prétend proposer une solution d'individualisation des clés. Le hic, c'est que l'on quitte la norme. […] A noter que les utilisateurs d'un réseau 802.11 voient leur débit utile réduit de 20% si le cryptage est réalisé par un logiciel. Il convient d'utiliser des cartes qui assurent le cryptage au niveau matériel. »

La technologie WiFi s'est rapidement répandue du fait de son faible coût principalement, mais aussi de l'assouplissement de la réglementation proposée par l'ART. De fait, il n'est plus surprenant de pouvoir se connecter à Internet avec WiFi dans les aéroports, les gares, les cafés (mais on cherche vainement des prises électriques car les batteries des ordinateurs portables ne permettent pas de dépasser quelques heures).

Si l'on souhaite relier son portable à Internet avec WiFi, il faut disposer d'un ordinateur (que nous supposons "fixe") déjà connecté à Internet de manière classique (Modem, ADSL, ...). On réalise alors une connexion point à point (liaison ad hoc) entre ces deux stations. Bien entendu, il faut équiper le portable et l'ordinateur fixe d'une carte WiFi. Cependant, la plupart des portables actuels sont déjà équipés de cette carte (notamment avec la technologie Centrino), mais ce n'est que rarement le cas des ordinateurs de bureau (le "fixe"). La carte WiFi coûte très peu ; elle peut s'insérer dans l'ordinateur (format PCI) ou être dans un boîtier extérieur. Le "fixe " sera paramétré en liaison partagée sur le Web.



Si l'on souhaite connecter plusieurs portables sur un fixe avec la méthode précédente, on aboutit à des difficultés de charge et il vaut mieux opter pour une connexion à un routeur WiFi lui même relié à Internet (on vend des routeurs WiFi munis de modem ADSL qui peuvent fonctionner en DHCP). On obtient alors un véritable réseau local sans fil.



WEP & Co

Le mécanisme initial de sécurité des transactions d'un dispositif Wifi est WEP (Wireless Equivalent Privacy). Décrivons ce mécanisme.

Il nécessite une clé secrète, introduite "manuellement" dans les stations devant communiquer entre elles dans un réseau Wifi. La clé secrète est donc fixée une fois pour toutes. Cette clé secrète comporte 5 ou 13 caractères. Comme chaque caractère (codé ASCII) correspond à 8 bits, le clé secrète a une longueur de 40 ou de 104 bits.

WEP ajoute à cette clé 3 caractères (24 bits) définis de manière aléatoire. Ces trois caractères constituent le "Initialization Vector" (IV). La clé complète (40+24 = 64 ou 104 + 24 = 128) est la concaténation de IV et de la clé secrète :

clé complète = IV + clé secrète = K

K est un vecteur correspondant à la chaîne de caractères formée par la clé complète : K[0] est le premier caractère de la clé complète, K[1] est le deuxième caractère de la clé complète, K[7] est le huitième caractère de la clé complète (et le dernier s'il s'agit d'une clé secrète de 40 bits).

On emploie ensuite la méthode RC4, méthode simple et rapide d'encryptage de données basée sur deux algorithmes : Key Scheduling Algorithm (KSA) et Pseudo Random Generation Algorithm (PRGA).

Intéressons-nous d'abord à KSA qui consiste à produire une séquence de caractères aléatoires. le code ASCII étendu étant sur 8 bits, on peut avoir 256 caractères différents. La séquence aléatoire envisagée est basée sur un tirage au hasard de ces 256 caractères. On commence par se donner une suite S[i] de i = 0 à i = 255 correspondant à tous les caractères : S[0] = 0, S[1] = 1, S[2] = 2, ..., S[255] = 255.

Puis on fabrique la clé complète de la manière suivante. Si la clé secrète est "MERCI" (codes ASCII 77, 69, 82, 67, 73), il faut trouver 3 autres caractères au hasard pour avoir la clé complète sur 8 bits qui sera donc XYZMERCI, où XYZ représentent les caractères tirés au hasard.

On effectue ensuite un mélange des S[i] par échanges répétés donnés par l'algorithme suivant

L'algorithme est donné ci-dessous avec le commentaire explicatif de chaque ligne

```
Pour i = 0 to 255
  j=j + S[i] + K[i]
  Echange de S[i] et de S[j]
FinPour
```

La valeur de K[i] est exprimée ici modulo 8, c'est à dire que K[8] = K[0], K[9] = K[1], etc. De même la valeur de j est exprimée modulo 256, c'est à dire que pour les valeurs supérieures à 255, comme par exemple j = 392 la valeur de j devient j = 392 - 256 = 36

Il faut maintenant passer à l'encryptage du texte. On utilise l'algorithme PRGA que nous ne décrirons pas ici. Signalons qu'il fait suite au mélande précédent de caractères, qu'il les mélange encore en les combinant avec les caractères du message.

Il a été montré que WEP n'était pas assez sûr.

Pour le remplacer, deux autres méthodes sont proposées : WPA (Wifi Protected Access) et WPA2. WPA est une méthode provisoire en attendant la norme 802.11i. WPA2 se réfère à cette norme. WPA et WPA2 fonctionnent sur toutes les cartes Wifi mais pas sur les points d'accès moins récents (avant 2003).

WPA reprend la méthode WEP mais en changeant de manière dynamique la clé secrète (qui était fixe dans WEP). WAP remplace aussi le CRC, considéré également comme peu sûr dans WEP, par une autre méthode dénommée MIC (Message Integrity Code) définie par un algorithme dénommé.....MIChaël qui inclut un compteur de trames.

WPA2 améliore WPA ; en particulier MIC est remplacé par .....MAC (Message Authentification Code) ! RC4 est également remplacé par AES (Advanced Encryption Standard).