1- Les Réseaux

Les réseaux informatiques

Avant propos

A l'heure où les réseaux domestiques se développent, ne serait-ce que parce que les PC ont une durée de vie courte et que c'est tout de même dommage de jeter une machine en état de marche, juste parce qu'elle a plus de trois ans, il devient intéressant de se pencher un peu plus sur le fonctionnement de cette chose, et d'en profiter pour élargir le débat aux réseaux locaux en général.

L'objectif de ce site est donc double:

- Etudier les dessous d'un réseau "local" (Local Area Network en anglo-saxon), en disant quelques mots à propos des réseaux d'entreprise (Wide Area Network); l'Internet n'étant finalement qu'une multitude de WAN interconnectés.
- En profiter pour construire, pourquoi pas, un réseau domestique, qui n'est finalement rien d'autre qu'un réseau local.

Bibliographie

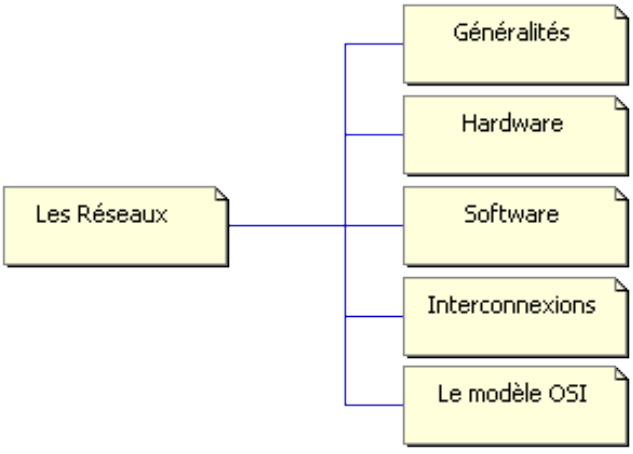
- A ceux qui vont arrêter ici leur lecture, parce qu'ils savent déjà tout ce qui va être dit.
- A ceux qui vont arrêter ici leur lecture, parce qu'ils croient déjà le savoir.
- A ceux qui auront lu ce chapitre et qui souhaitent en savoir plus.

je conseillerai vivement la lecture de deux ouvrages qui sont des références dans ce domaine:

- **"Réseaux, Architectures, protocoles, applications"**
  De Andrew Tanenbaum
  Chez InterEditions
- **"Les réseaux"**
  De Guy Pujolle
  Chez Eirolles

Normalement, peu de gens survivent à la lecture de ces deux pavés, mais ce n'est pas interdit d'essayer quand même... Ceux qui ont déjà réussi cet exploit peuvent aller se reposer tout de suite, ils n'apprendront effectivement rien ici.

Un plan pour mieux s'y retrouver...



2- Généralités

Petite histoire...

Autrefois, l'informatique était centralisée. De grosses machines travaillaient en temps partagé pour plusieurs utilisateurs. Ces utilisateurs avaient à leur disposition des "terminaux bêtes" dont un bon exemple serait le MINITEL.

Les ordinateurs "mainframes" pouvaient être reliés entre eux par des réseaux, l'un des premiers en France étant "Renater" un réseau reliant les facultés et centres de recherche.

Puis arrive l'ère de l'ordinateur personnel. Bien plus souple d'emploi. Chacun dispose du sien et peut en faire ce que bon lui semble. Mais cette puissance personnelle est isolée. Les utilisateurs ne peuvent plus partager leur données.

Les "informaticiens" regardent ces jouets d'un œil amusé, considérant que le "Personal Computer" n'a rien à faire dans le paysage informatique "sérieux"...

Mais cette isolement ne va pas durer. L'informatique prend toute sa valeur lorsque les informations traitées sont facilement communicables. Il faut réinventer le réseau, afin de connecter les ordinateurs personnels entre eux. Les constructeurs de PC s'y attellent, principalement avec IBM et Microsoft qui proposent LAN Manager et NetBEUI. Il s'agit d'une couche réseau rudimentaire mais déjà fonctionnelle sous MS DOS. Novell propose sa solution propriétaire IPX/SPX, également pour PC. De son côté Apple développe pour ses machines une solution également propriétaire: "Apple Talk"

De l'autre côté de la barrière, les "vrais ordinateurs" fonctionnent sous des OS eux aussi propriétaires, mais le réseau existe. Un système d'exploitation se développe: Unix. Chaque constructeur propose sa version, mais tous savent communiquer entre eux par le protocole TCP/IP.

Aujourd'hui? Un PC "bas de gamme" est souvent plus puissant que bien des "mainframes" d'il y a 30 ans... Tous les OS sont orientés réseau et proposent un protocole TCP/IP qui leur permet de communiquer.

Allez, pour faire rêver mes lecteurs les plus "anciens", lorsque j'étais à la fac (les années 70), le centre de calcul de Saint Jérôme disposait d'un IBM 1130, certes pas un "mainframe", juste un mini ordinateur: 3 disques durs de 5 Mo (!), 8 KWords de RAM (tores de ferrite), mais des Mots de 16 bits quand même... Si, si, vous avez bien lu. Un Apple II faisait mieux.

Celui que vous voyez à côté est la version "de base". Un seul disque dur et le minimum de mémoire de masse: 2 KWords... Notez l'absence d'écran, remplacé par un télétype à boule, bruyant et d'une grande lenteur. Sur le côté droit, observez la bande de papier perforée, pour l'archivage des données...

Pourquoi un réseau?

Toute personne ayant travaillé sur un réseau ne pourra plus s'en passer. Témoin l'extraordinaire explosion de l'Internet. Parmi les avantages les plus flagrants, citons:

- L'extrême facilité avec laquelle il est possible de communiquer des informations à son entourage
- La simplicité avec laquelle un utilisateur peut changer de poste de travail sans pour autant devoir transporter ses fichiers sur disquette ou autre support de stockage.

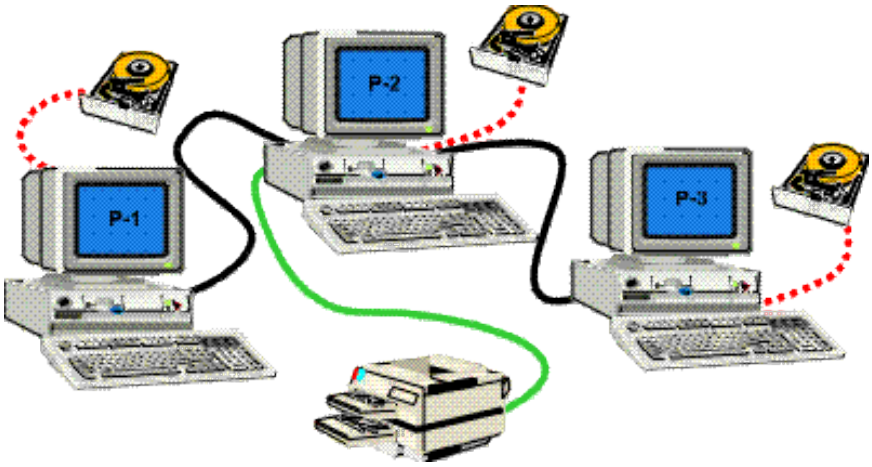
Les concepts des réseaux locaux

Un réseau, nous l'avons compris, permet de connecter des ordinateurs entre eux. Mais les besoins sont très divers, depuis le réseau domestique ou d'une toute petite entreprise jusqu'aux réseaux des grandes sociétés.

Voyons deux approches fondamentalement différentes, encore que l'une peut facilement évoluer vers l'autre.

Le "Peer to Peer"

Principe



- Les postes de travail sont simplement reliés entre eux par le réseau. Aucune machine ne joue un rôle particulier. Chaque poste peut partager ses ressources avec les autres postes.
- C'est à l'utilisateur de chaque poste de définir l'accès à ses ressources. Il n'y a pas obligatoirement d'administrateur attitré.
- Dans l'exemple, chaque poste peut partager tout ou partie de sa mémoire de masse, le poste P-2 peut partager son imprimante.

Avantages

Il y en a quelques uns...

- Il est facile de mettre en réseau des postes qui étaient au départ isolés.
- Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.
- Dans un groupe de travail, l'imprimante peut être utilisée par tous.

Cette méthode est pratique et peu coûteuse pour créer un réseau domestique

Inconvénients

Il y en a beaucoup!

- Chaque utilisateur a la responsabilité du fonctionnement du réseau.
- Les outils de sécurité sont très limités.
- Si un poste est éteint ou s'il se "plante", ses ressources ne sont plus accessibles
- Le système devient ingérable lorsque le nombre de postes augmente.
- Lorsqu'une ressource est utilisée sur une machine, l'utilisateur de cette machine peut voir ses performances diminuer.

Conclusions

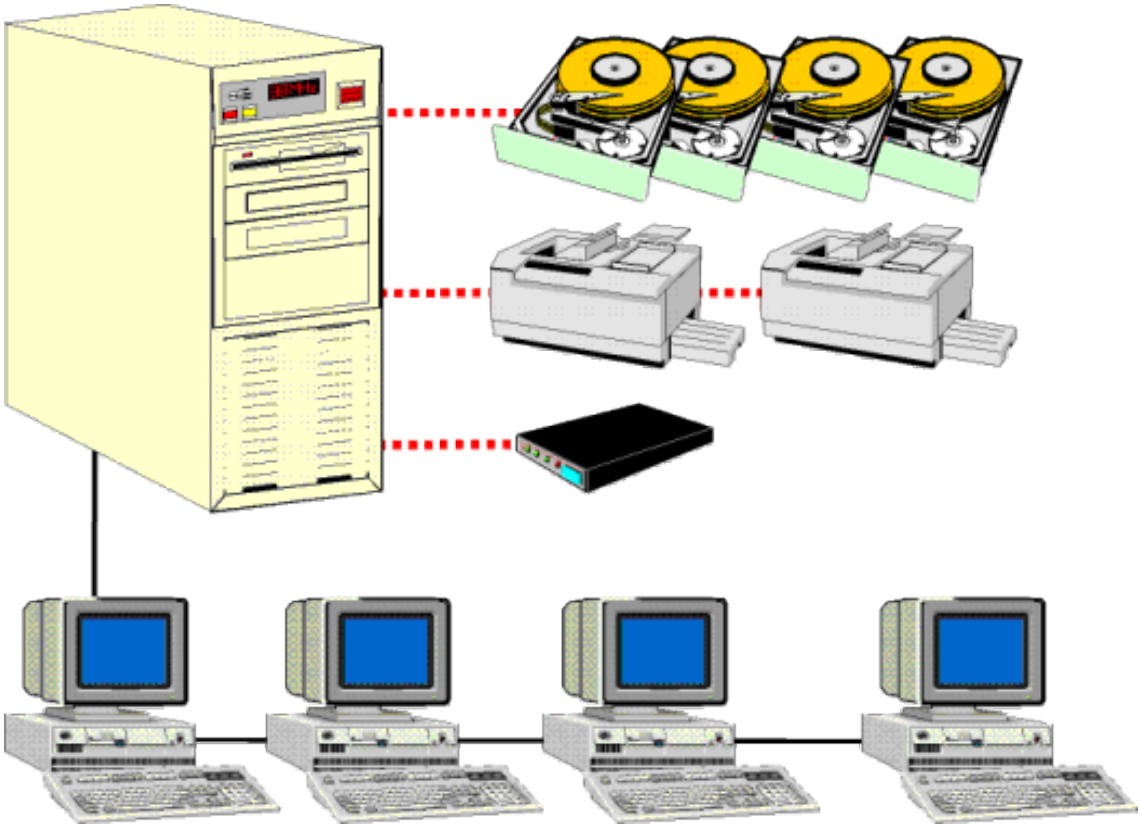
Ce type de réseau n'offre de réel intérêt que dans une configuration particulière:

- Les postes sont peu nombreux (pas plus d'une dizaine).
- Les utilisateurs restent attachés à un poste dont ils sont responsables.

Le "Client / Serveur"

Principe

Positionnez le curseur sur la zone souhaitée pour avoir la légende.



- Les ressources réseau sont centralisées.
- Un ou plusieurs serveurs sont dédiés au partage de ces ressources et en assurent la sécurité
- Les postes clients ne sont en principe que des clients, ils ne partagent pas de ressources, ils utilisent celles qui sont offertes par les serveurs.

Avantages

Il y en a beaucoup...

- Les serveurs sont conçus pour le partage de ressources et ne servent pas de station de travail. Il suffit de les dimensionner en fonction de la taille du réseau et du nombre de clients susceptibles de s'y connecter.
- Les systèmes d'exploitation de serveurs proposent des fonctions avancées de sécurité que l'on ne trouve pas sur les réseaux "peer to peer".
- Ils proposent également des fonctions avancées à l'usage des utilisateurs

Inconvénients

Il y en a quelque-uns tout de même...

- La mise en place d'un tel réseau est beaucoup plus lourde qu'un cas simple de "poste à poste"
- Elle nécessite **Impérativement** la présence d'un administrateur possédant les compétences nécessaires pour faire fonctionner le réseau.
- Le coût est évidemment plus élevé puisqu'il faut la présence d'un ou de plusieurs serveurs.
- Si un serveur tombe en panne, ses ressources ne sont plus disponibles. Il

comme par exemple les profils itinérants qui permettent à un utilisateur (sous certaines conditions) de retrouver son environnement de travail habituel, même s'il change de poste de travail.
- Les serveurs étant toujours en service (sauf en cas de panne...), les ressources sont toujours disponibles pour les utilisateurs.
- Les sauvegardes de données sont centralisées, donc beaucoup plus faciles à mettre en oeuvre.
- Un administrateur gère le fonctionnement du réseau et les utilisateurs n'ont pas à s'en préoccuper

faut donc prévoir des solutions plus ou moins complexes, plus ou moins onéreuses, pour assurer un fonctionnement au moins minimum en cas de panne.

Conclusions

Ce type de réseau est évidemment le plus performant et le plus fiable. Vous l'aurez compris, ce n'est pas la solution la plus simple pour un réseau domestique, c'est cependant ce type d'architecture que l'on retrouve sur les réseaux d'entreprise, qui peut parfaitement supporter plusieurs centaines de clients, voire plusieurs milliers.

Et pour aller plus loin...

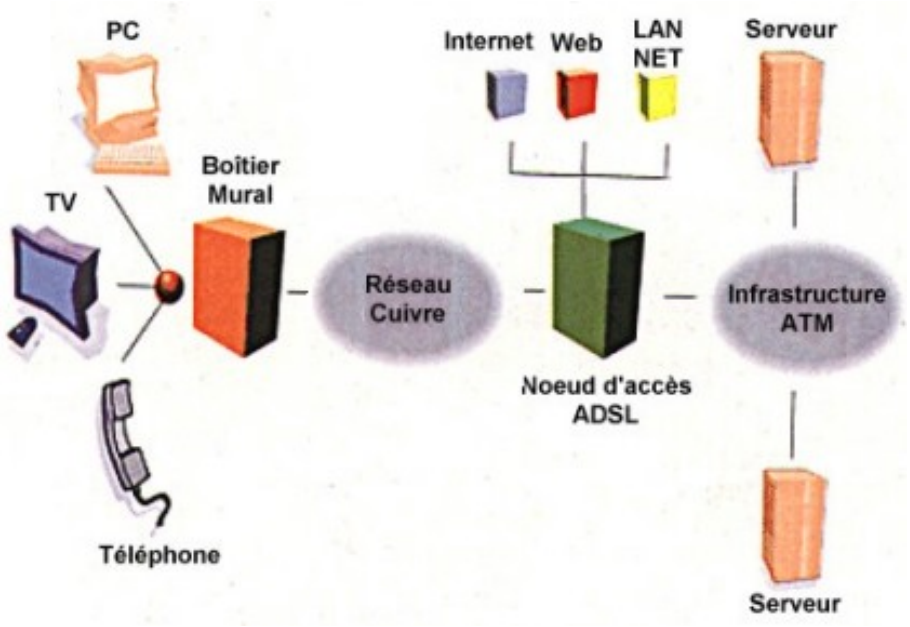
Par définition, un réseau local s'étend sur une petite surface (un câblage simple peut rarement dépasser quelques centaines de mètres). Les entreprises doivent souvent créer des réseaux beaucoup plus grands.

La fibre optique permet des distances plus importantes, mais il n'est pas facile, même s'il devient possible d'obtenir les autorisations nécessaires, de creuser des tranchées dans le domaine public pour passer son réseau. Dans ces cas là, il reste tout de même plus simple de faire appel aux services d'entreprises spécialisées, France Télécom par exemple. Le moyen le plus rudimentaire et le moins performant étant d'utiliser une ligne téléphonique analogique avec un modem à chaque bout. (Ne rigolez pas, certaines connexions entre "gros ordinateurs" se faisaient avec des modems RTC à 9600 bps i n'y a pas si longtemps).

Il est clair que les besoins actuels sont sans commune mesure. Les opérateurs de communications en sont à ce point convaincus qu'ils déploient des efforts énormes pour augmenter leur capacités de transport d'informations. Des centaines de kilomètres de câble ou de fibre optique sont mis en place chaque jour dans le monde, le long voies ferrées, des autoroutes, à côté des conduites d'eau et d'électricité. Des projets de communication par satellites en orbite basse sont en cours de réalisation malgré les déboires connus du projet "Iridium" et les canaux hertziens ne sont pas délaissés non plus. Tout cela pour faire de la téléphonie bien sûr, mais également pour offrir des "tuyaux" pour les réseaux informatiques à venir.

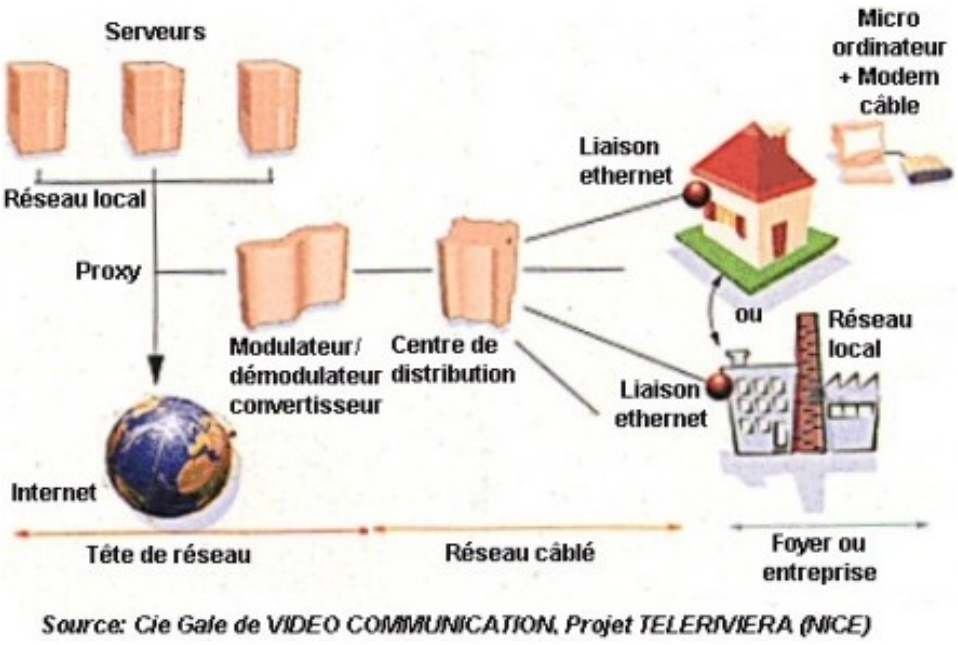
Quelques technologies "au goût du jour"...

En plus des "LS", Lignes spécialisées dont le prix de la location est totalement hors de portée d'un particulier, voire d'une petite entreprise, d'autres solutions existent. Il n'est pas question les les détailler ici, voyons tout de même les possibilités de connexion à l'Internet "haut débit" actuellement accessibles.



La technologie "ADSL" qui permet, en utilisant les structures téléphoniques actuelles de transmettre de l'information à haut débit. Non seulement la téléphonie "classique" mais aussi les données numériques.

Le câble télévision, qui n'a jusqu'à ce jour connu qu'un intérêt très limité, fortement concurrencé par les satellites.



Source: Cie Gale de VIDEO COMMUNICATION, Projet TELERIVIERA (NICE)

Le câble pourrait bien cependant survivre grâce à la distribution de données numériques interactives.

Dans le domaine de l'Internet à haut débit, il semble bien que le câble ne soit pas en état de rivaliser avec l'ADSL. Bien que la technologie fonctionne maintenant correctement, le problème du volume de données en voie remontante (upload) paraît être insoluble, obligeant les câblo opérateurs à imposer des limites aux

volumes d'upload des
abonnés.

Dans l'illustration ci dessus, il est dit que la liaison entre le centre de distribution et l'utilisateur final est une liaison Ethernet, ce serait plutôt actuellement de l'ATM.

La boucle locale radio, qui, pour l'instant, semble revoir fortement ses ambitions à la baisse et se cantonner à des offres proches des lignes spécialisées.

3- Hardware

Un réseau informatique, c'est comme tout ce qui est informatique: il y a du matériel et du logiciel pour le faire fonctionner...

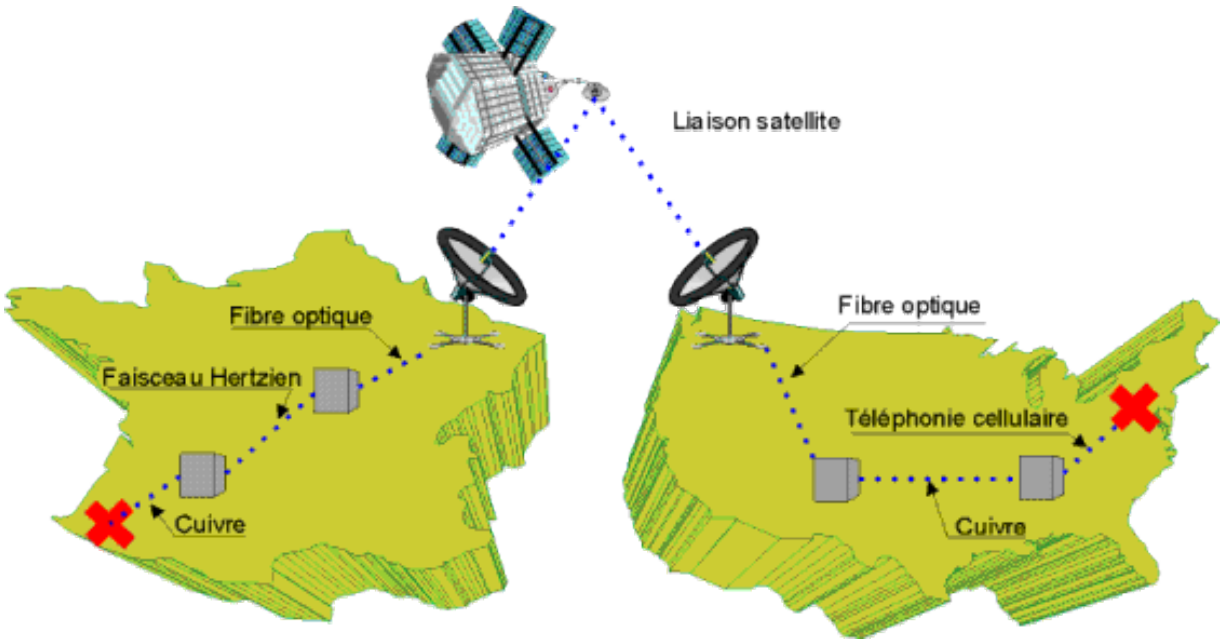
Le matériel peut se décomposer en sous-groupes:

Les médias de transport

Dans les médias de transport, nous trouvons:

- **Les câbles en "cuivre"** (qui peuvent en fait être construits avec n'importe quel métal bon conducteur). C'est en général le média le moins coûteux, mais également le plus limité, surtout en terme de distance.
- **Les fibres optiques** qui ont l'avantage d'être insensibles aux perturbations électromagnétiques dans lesquelles nous baignons. De plus, la vitesse de propagation de la lumière dans ces fibres autorise de longues distances et de nombreuses solutions permettent une très grande bande passante, donc un gros débit de données.
  Malheureusement, la fibre optique souffre de quelques défauts:
  - Sa relative fragilité.
  - La difficulté d'y adapter de la connectique
  - Le prix de cette connectique.
- **Les liaisons "hertziennes"** qui couvrent elles-mêmes plusieurs technologies:
  - La liaison "classique" c'est à dire en émission omnidirectionnelle qui encombre beaucoup l'espace mais apporte une grande souplesse dans la mobilité des équipements connectés.
    Un exemple typique en est le téléphone mobile dit "cellulaire". Une telle technologie pourra (un jour) aisément transporter des données numériques pour des connexions mobiles.
  - La liaison par faisceau hertzien plus intéressante car l'émission est extrêmement directive. L'inconvénient est que les émetteurs et les récepteurs doivent être rigoureusement alignés et ne peuvent donc pas être mobiles.
  - Les liaisons par satellite. Ces dernières peuvent utiliser:
    - Des satellites géostationnaires qui sont placés à très haute altitude et au dessus de l'équateur. Il faut en effet trouver des orbites telles que la vitesse de maintien aboutisse à une vitesse angulaire identique à celle de la rotation de la terre et que les deux rotations se fassent autour du même axe.
      Ces satellites sont bien adaptés pour la télévision non interactive, dans ce cas le récepteur peut être placé directement chez le client. Ils peuvent également servir de relais pour la téléphonie intercontinentale.
      Cependant, la distance à parcourir est très grande et un retard perceptible est introduit dans la transmission des données, ce qui perturbe la téléphonie et introduit un temps de latence non négligeable dans les transmissions informatiques (ping).
      La puissance nécessaire à l'émission vers le satellite est telle que le particulier ne peut y avoir accès, raison pour laquelle l'interactivité est impossible par ce moyen seul.
    - Des satellites à basse altitude qui ne sont pas géostationnaires, mais qui, s'il sont bien répartis, peuvent assurer une retransmission "sans trous". L'avenir de cette technologie est actuellement assez précaire (voir le projet "Iridium")

Il est courant, pour aller d'un point à un autre, d'emprunter plusieurs de ces technologies...



Les Interfaces avec les ordinateurs

Le rôle de cette interface est fondamental:

L'aspect physique

Il faut assurer la continuité du passage des données entre le média du réseau et le bus de données de l'ordinateur. Mais ce média peut être:

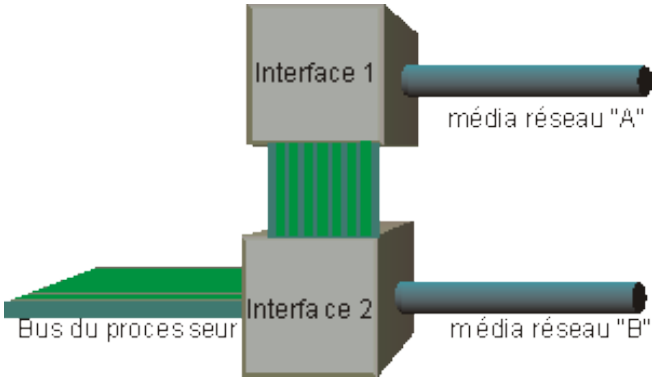
- Une fibre optique
- De la paire torsadée
- Du câble coaxial
- Une onde hertzienne
- Un faisceau lumineux infrarouge...

L'aspect Logique

L'interface est étroitement liée au niveau 1 du modèle O.S.I. Son "firmware" doit donc tenir compte des spécifications de la norme, afin de pouvoir supporter les couches supérieures (c'est-à-dire les divers protocoles réseau). En d'autres termes, cette interface doit apporter une complète indépendance entre les logiciels réseau et le support matériel utilisé.

Les passerelles entre réseaux

Il existe une multitude de "passerelles" entre réseaux. D'une manière générale, une passerelle permet la communication entre deux réseaux distincts qui peuvent être aussi différents que possible. Chaque passerelle sera adaptée au besoin spécifique.



Sans entrer ici trop dans le détail, on peut considérer une passerelle quelconque comme étant un ordinateur muni de plusieurs interfaces, une pour chaque réseau, avec un logiciel capable de faire transiter les informations d'un réseau vers l'autre lorsque c'est nécessaire.

Des informations plus précises sont données au chapitre "interconnexions"

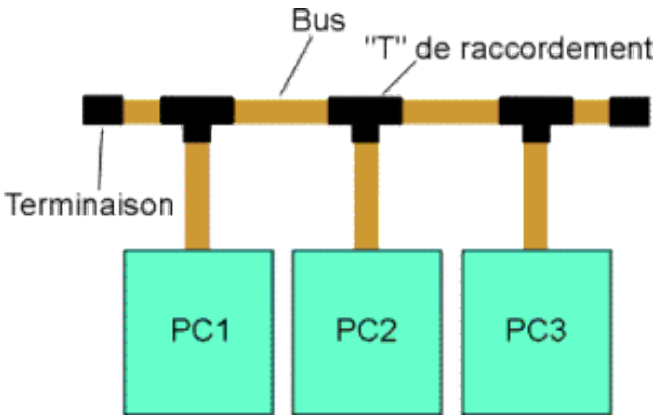
Dans notre rayon d'action, seul le cuivre va nous être accessible (l'onde Hertzienne également avec le protocole 802.11 qui permet la construction d'un réseau local sans fil, mais c'est quand même nettement plus cher).

Les moyens disponibles pour le câblage d'un réseau local

Il est sous entendu que nous allons construire un réseau Ethernet utilisant des câbles en cuivre. Nous verrons plus loin ce que cela veut dire. Deux technologies sont actuellement accessibles.

Le BUS

Principe

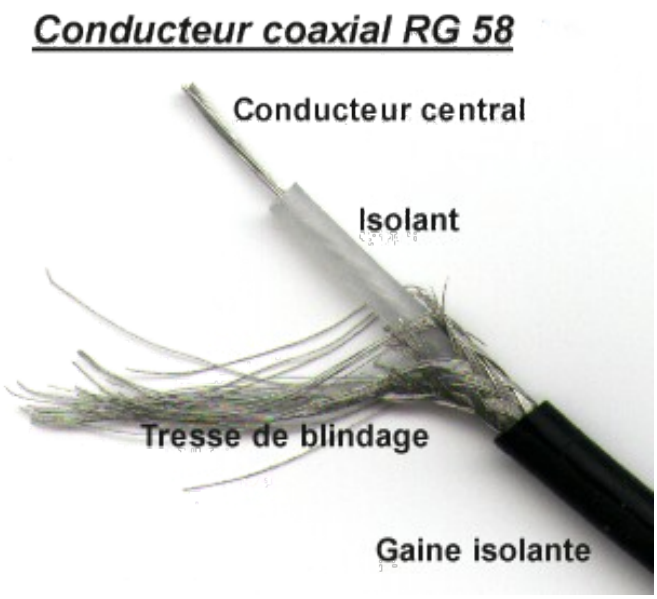


Le principe du "BUS" est extrêmement simple:

- Un conducteur unique représente le réseau.
- Chaque extrémité est bouclée sur un "bouchon" dont l'impédance électrique est égale à l'impédance caractéristique du conducteur, ceci afin d'éviter les réflexions des signaux en bout de câble.
- Chaque poste est "piqué" sur ce bus au moyen d'un "T" de raccordement.

Le technologie présentée ci-dessous est adaptée aux petits réseaux.

Pratique



Dans ce cas de figure, le câble le plus souvent utilisé est du coaxial de type RG58. Il est souple, fin et relativement facile à mettre en œuvre.

Le câble RG58, bien connu de ceux qui ont tâté de la CB, présente une impédance caractéristique de 50 Ohms

Les prises de type "BNC" sont facilement montées si l'on dispose de la pince à sertir adéquate.

Le "T" de type BNC permet les raccordements, avec son type de prise à verrouillage par baïonnette.

Le bouchon de terminaison, également de type BNC, se trouve aisément dans le commerce, au même titre d'ailleurs que les autres accessoires décrits plus haut.

Au final, il est très simple et rapide de connecter entre eux quelques PC par ce moyen.

Avantages

Il n'y a qu'un seul avantage à utiliser cette technologie, mais il est de taille:

- Après avoir vu les divers constituants, il devient évident que ce procédé est peu coûteux, facile et rapide à mettre en œuvre.

Inconvénients

Ils sont hélas nombreux:

- Lorsque le réseau dépasse les dimensions d'une pièce, il faut alors passer les murs, ce qui "fige" considérablement la topologie et diminue les possibilités d'extension.
- Si un défaut de connectique apparaît, c'est tout le réseau qui devient inopérant. En effet, tout se passe alors comme si l'on avait deux réseaux, mais chacun d'eux ayant une extrémité non adaptée. Plus rien ne fonctionne et le défaut n'est pas toujours visible. Les investigations sont longues et laborieuses.

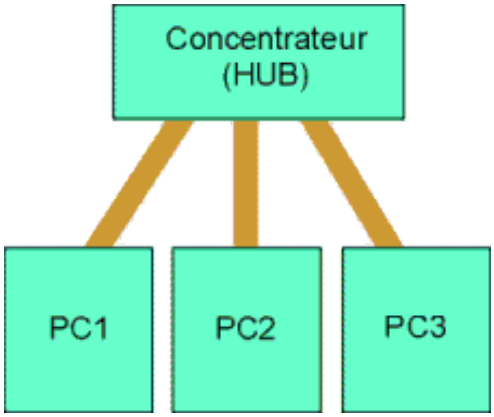
Conclusions

Malheureusement, ce type de réseau est limité à 10 Mbits/s et n'a plus d'avenir, bien qu'encore suffisant pour un réseau domestique.

Il devient de plus en plus difficile de trouver ce genre d'adaptateur réseau. Les derniers modèles encore vendus sont souvent de type "combo", c'est à dire qu'ils permettent aussi bien un câblage coaxial en BUS qu'un câblage en étoile avec des paires torsadées, comme nous allons le voir tout de suite. Naturellement, un seul de ces deux modes est utilisable pour une interface donnée.

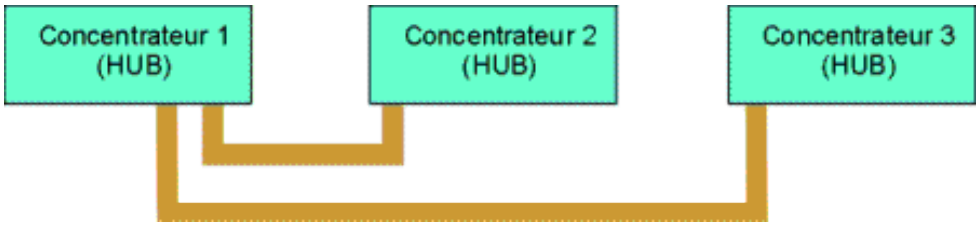
L'étoile

Principe

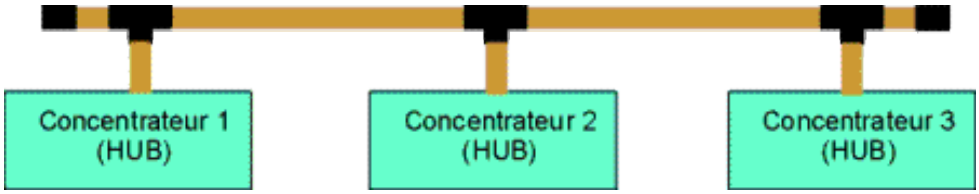


Chaque PC est relié par un câble constitué de 4 paires torsadées (dont deux seulement servent, normalement, l'une pour l'émission et l'autre pour la réception) à un concentrateur, encore appelé "HUB".

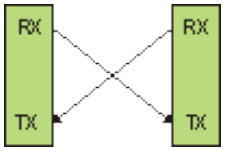
Les HUBS peuvent être "cascadés" en utilisant un média de type "paires torsadées": Normalement, il ne peut y avoir qu'un seul niveau de cascade. Autrement dit, sur l'illustration ci dessous, il ne devrait pas y avoir de hubs cascadés sur les hubs 2 et 3.



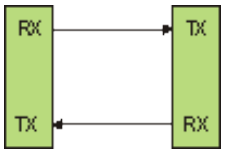
Ou montés sur un BUS, en utilisant un média de type "coaxial" ou "fibre optique":



Sur de la paire torsadée, chaque paire est unidirectionnelle. Un petit schéma fera mieux comprendre:



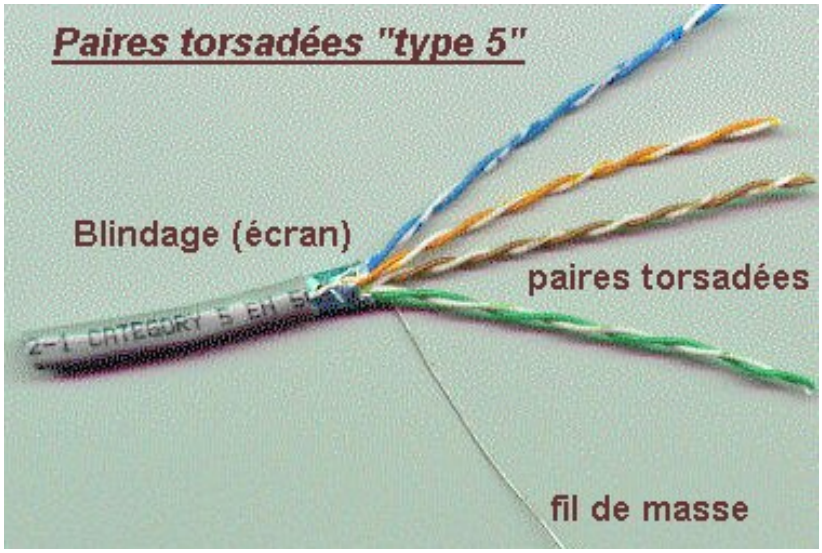
Deux équipements connectés doivent faire correspondre le TX (Emission) de l'un au RX (Réception) de l'autre. Normalement, il faudrait donc des câbles croisés. C'est ce qui est nécessaire si l'on souhaite relier directement deux PC entre eux.



Mais si l'on s'arrange pour que l'un des équipements ait sa prise déjà croisée, alors, il faut un câble droit. Les HUBS ont leurs prises croisées, c'est pour cela qu'il y a un X marqué sur ses prises. Il faut donc un câble droit pour connecter un PC à un HUB.

Notez que les équipements récents (HUBS et Swiths) sont capables de détecter automatiquement les signaux d'entrée et de sortie présents sur la prise et réagissent en conséquence. Autrement dit, l'équipement découvrira automatiquement s'il est nécessaire de croiser ou non.

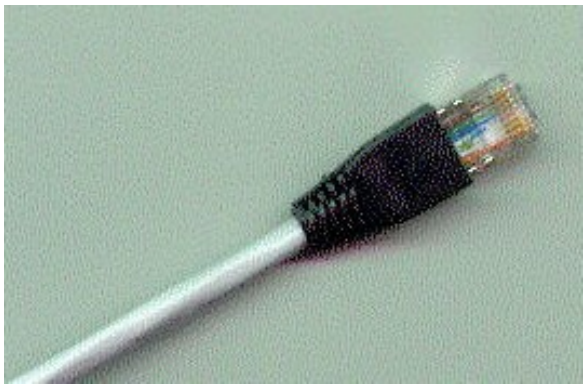
Pratique



Le câble de type 5 est constitué de 4 paires torsadées. il peut être blindé (écranté) ou non.

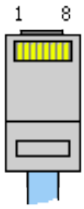
Le type 5 est certifié pour les réseaux 100 Mb/s. Le câble écranté offre une meilleure immunité au bruit électronique, il est à utiliser de préférence, même si son coût est plus élevé.

Ce type de câble est terminé par des connecteurs "RJ45". Suivant qu'un blindage existe ou non sur le câble, le connecteur est à choisir en conséquence. Il se place simplement si l'on dispose d'une pince spécialement conçue pour cet usage



Câblage

Bien qu'il ne soit pas intéressant de réaliser soi-même son câblage, d'abord à cause du prix de l'incontournable pince à sertir et ensuite à cause de la plus faible résistance des prises par rapport à celles qui sont moulées en usine, voici le plan de câblage, conforme à la norme EIA568B, pour une prise non croisée.



La prise est vue du côté des points de contact

1	**TX +**	Transmission de données +	Blanc/Orange
2	**TX -**	Transmission de données -	Orange
3	**RX +**	Réception de données +	Blanc/Vert
4	**1+**	Non utilisé en 10/100 BT	Bleu
5	**1-**		Blanc/Bleu
6	**RX -**	Réception de données -	Vert

7	**2+**	Non utilisé en 10/100BT	Blanc/Marron
8	**2-**		Marron

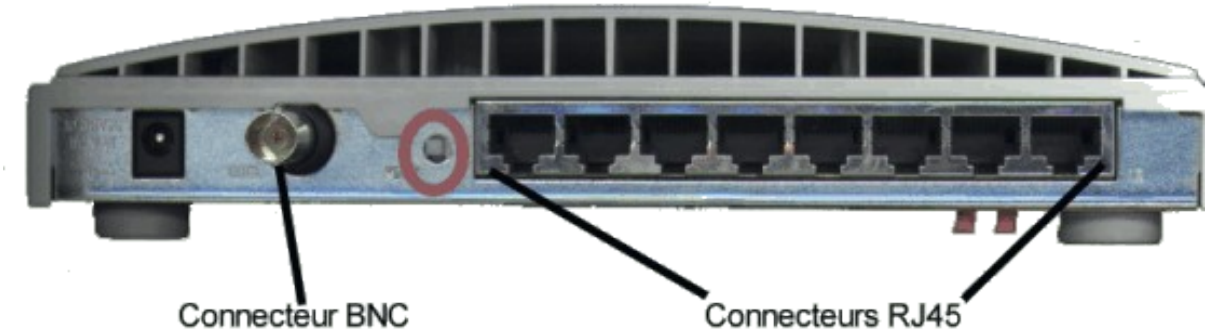
Ce qu'il est fondamental de comprendre, c'est que les paires sont torsadées pour augmenter l'immunité au bruit (rayonnement en mode commun). Il est donc nécessaire de respecter l'intégrité de ces paires:

- TX+ et TX- doivent être câblés avec les fils d'une même paire
- RX+ et RX- également.

Lorsque l'on utilise un câble écranté, il faut également utiliser des prises blindées. Le fil de blindage du câble est à mettre en contact avec le blindage de la prise.

Il faut également remarquer que, si la paire TX utilise les broches 1 et 2, la paire RX utilise, elle, les broches 3 et 6 (non contiguës). En ce qui concerne le code des couleurs, c'est moins fondamental. Son seul intérêt est de normaliser.

Voici un exemple de HUB 10 Mb/s: Il possède huit ports de type RJ 45 et un port BNC, permettant un montage sur un BUS RG58. De marque "3COM" (sans aucune intention publicitaire).



Notez le petit bouton en face arrière qui nécessite quelques explications. Nous avons vu que pour connecter deux équipements entre eux, il faut faire correspondre le RX de l'un au TX de l'autre, raison pour laquelle les prises des HUBs sont croisées et marquées d'un X.

Seulement voilà, lorsque l'on cascade des HUBs avec de la paire torsadée, si les deux prises sont croisées, ça ne va plus parce que les deux croisements s'annulent. Sur ce modèle de HUB, il y a une prise particulière que l'on peut à volonté croiser ou non au moyen de ce petit poussoir. Normalement, tout HUB dispose d'un moyen d'être cascadé et offre donc une prise non croisée. Sur les modèles d'entrée de gamme, il y a une prise dédiée non croisée. Sur d'autres modèles, il y a un port disposant de deux prises: L'une croisée, l'autre non. Dans ce cas, il ne faut pas oublier que les deux prises étant reliées au même port, une seule des deux peut être utilisée.

La face avant de ce HUB donne des informations concernant l'état de chaque port, la densité du trafic sur le réseau et même les "collisions".

Avantages

- D'un fonctionnement beaucoup plus sûr que le bus, si un lien vient à se rompre, seul le PC connecté par ce lien est absent du réseau.
- Il est aisé d'ajouter des postes au réseau, même s'ils sont dans une pièce.
- Cette technologie permet de réaliser un réseau 100 Mbits/s (à condition de disposer de HUBS qui savent le faire).

Inconvénients

- La longueur totale de câble mise en œuvre est importante.
- Au voisinage du HUB, on obtient un faisceau de câbles imposant.
- Le coût est tout de même plus élevé que dans une architecture BUS.

Et les "switchs" ?

Pour l'instant, contentons nous de dire que c'est presque la même chose qu'un HUB. Ce n'est pas vrai dans son mode de fonctionnement, nous le verrons plus loin, mais ça l'est au niveau de la topologie du réseau.

Conclusions

L'exemple est fourni pour un petit réseau. Cependant, il existe des HUBS 100 Mb/s de 8, 12 ou 24 ports, que l'on peut monter en BUS sur une fibre optique, autorisant des réseaux à haut débit et de très grande taille.

De plus, des concentrateurs plus performants appelés "switches" permettant une meilleure répartition de la bande passante du réseau et augmentant encore les capacités de ce dernier. Ces composants s'apparentent aux ponts qui sont détaillés dans le chapitre "routage".

4- Software

Présentation

La partie purement logicielle est bien évidemment indispensable.

Si nous voulions refaire un parcours initiatique, après avoir construit la structure matérielle du réseau, nous pourrions faire démarrer deux postes sous MS DOS 6.2 par exemple, et constater que le réseau ne sert à rien. Il faudrait ajouter non seulement les drivers des adaptateurs réseau, mais encore la couche logicielle nécessaire à la communication. Si cette étape peut être menée à bien et qu'il reste toujours un peu de mémoire disponible (MS DOS ne sachant gérer que 640 Ko, ne laissant au mieux qu'un peu plus de 500 Ko pour l'utilisateur, alors la suite des commandes "net xxx" peut être utilisée.

Cette manipulation n'a de réel intérêt que pour les archéologues de l'informatique. Lorsque les réseaux locaux ont commencé à se généraliser, Windows existait déjà dans sa version 3.10 et il existait une mise à niveau permettant de mettre en oeuvre un réseau NetBEUI et même IPX/SPX, pour la connectivité avec Novell qui, à cette époque, avait une avance assez considérable.

Les couches réseaux ont été intégrées nativement à Windows à partir de la version 3.11, parallèlement à la sortie des premières versions Windows NT.

Deux problèmes à résoudre

C'est bien de disposer d'un ensemble de postes connectés entre eux, encore faut-il établir des protocoles pour transmettre les données avec quelques espoirs d'efficacité. Des protocoles, nous allons en voir quelques uns et à tous les étages. Mais commençons par le niveau le plus bas, sur le câble lui-même.

Parler et se faire entendre...

Contrairement à la téléphonie qui met en œuvre une liaison "point à point", il n'y a en général que deux interlocuteurs en ligne, un réseau informatique met toutes les machines connectées sur la même ligne. Il faut donc trouver un moyen pour que celui qui parle soit entendu. Il y a plusieurs méthodes pour organiser une telle assemblée, nous allons en voir trois:

La liberté dans l'auto discipline

Il s'agit du système ETHERNET (à ne pas confondre avec INTERNET). Ici, un poste qui doit émettre commence par écouter le réseau. Si personne n'est en train de parler, il émet une trame de données. Comme chaque poste s'assure qu'il y a le silence avant de prendre la parole, les choses se passent en général bien.

Cependant, lorsqu'il y a beaucoup de postes, il peut se faire que deux postes décident d'émettre en même temps; il y a alors une collision entre les deux trames émises et les données deviennent inutilisables. ETHERNET utilise donc un système de détection de

collision. Dans un tel cas, chaque poste attendra un temps aléatoire et refera une tentative.

C'est le procédé le plus employé dans les réseaux actuels. celui que nous utiliserons sur un réseau local.

Avantages

Lorsqu'il y a peu de trafic sur le réseau, il n'y a pas de perte de temps et les communications sont très rapides.

Les médias mis en œuvre sont simples (paires torsadées ou coaxial) et peu onéreux, de même que la connectique.

Inconvénients

Lorsque le taux de collision devient important, le réseau perd beaucoup de temps à transporter des informations inutilisables et le rendement diminue, la bande passante étant alors consommée par les collisions.

Une autre caractéristique peut devenir un inconvénient: Il est impossible de déterminer le temps qu'il faudra pour être sûr qu'un poste a pu parler à un autre, ce temps pouvant être très court s'il y a peu de trafic ou beaucoup plus long s'il y a beaucoup de collisions.

L'organisation déterminée

C'est le protocole "Token Ring" (Anneau à jeton).

Pour parler, il faut avoir le jeton. Le réseau est constitué comme un anneau sur lequel un contrôleur passe un jeton à chaque hôte connecté, à tour de rôle. Ne peut émettre que celui qui dispose du jeton.

Avantages

Dans un tel système, il ne peut pas y avoir de collisions, c'est l'ordre parfait.

Il est parfaitement possible, si l'on connaît le nombre de postes sur le réseau, de connaître le temps maximum qu'il faudra pour qu'un poste puisse parler à un autre. (intéressant dans la gestion d'événements "en temps réel").

Inconvénients

Il est difficile de construire une vraie boucle! En fait, le retour se fait dans le même câble. La connectique est donc plus complexe et onéreuse.

Enfin, une solution chère mais efficace

Le réseau ATM, mis au point par les opérateurs de télécommunications, est un procédé complexe et coûteux, mais qui garantit un fonctionnement fluide et une bande passante déterminée pour chaque poste du réseau; conditions indispensables pour effectuer de la téléphonie ou de la télévision, phénomènes en temps réel s'il en est!

Ces réseaux fonctionnent comme des réseaux commutés. Un chemin virtuel est établi entre les deux postes qui veulent échanger des données. ATM fera peut-être un jour l'objet d'un chapitre dans ce site...

Utiliser le même langage

Une fois que l'on s'est mis d'accord sur la façon d'organiser les échanges, il faut adopter un langage commun. Il existait beaucoup de langues aux débuts des réseaux (en gros, une par constructeur). Aujourd'hui, il en reste moins.

Protocoles populaires:

NetBEUI

Développé par Microsoft et IBM à l'époque des premiers réseaux de PC, ce protocole simplissime fonctionne très bien sur de petits réseaux. Malheureusement, son efficacité décroît avec le nombre de postes. De plus, il n'est pas "routable", ce qui fait que l'on ne peut interconnecter des réseaux NetBEUI autrement que par des ponts.

IPX/SPX

Développé par la société NOVELL, qui s'est octroyée la part du lion dans les premiers réseaux de PC avant que Microsoft ne développe Windows NT. Plus efficace que NetBEUI pour les gros réseaux, ce protocole est de plus routable ce qui augmente les possibilités d'interconnexions.

TCP/IP

Développé dans le monde UNIX, ce protocole est de très loin le plus compliqué. Cependant, il a été conçu au départ pour l'interconnexion de réseaux (IP=Internet Protocol!).

C'est le protocole le meilleur pour les gros réseaux et il est incontournable pour l'usage d'Internet. C'est **LE** standard actuel.

5- Interconnexions

Objectifs

Les réseaux informatiques ont pris une telle importance qu'il devient de plus en plus nécessaire de les interconnecter. C'est d'ailleurs le rôle fondamental de l'INTERNET, même si l'on peut très bien imaginer plusieurs "INTERNETS" parallèles...

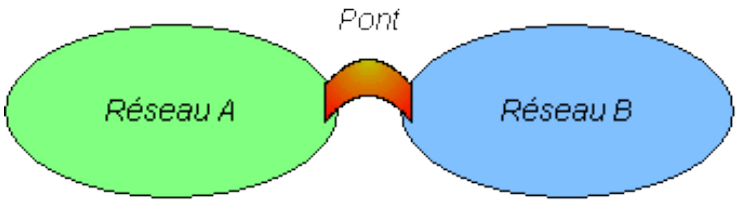
Prenons un exemple simple: Une entreprise disposant de plusieurs succursales, chacune équipées d'un réseau, peut vouloir interconnecter ces réseaux.

Plus simplement, un organisme comportant plusieurs secteurs d'activité pourrait disposer d'un réseau spécifique pour chaque activité, tous ces réseaux pouvant être interconnectés pour une meilleurs distribution de l'information.

Sans entrer dans les détails des médias pouvant être utilisés pour transporter l'information d'un réseau à l'autre, nous allons ici énumérer quelques "passerelles" classiques.

Les outils d'interconnexion

Les ponts



Ils sont utilisés pour interconnecter deux réseaux utilisant le même protocole, par exemple NetBEUI sur éthernet. Les ponts travaillent au niveau de la couche 2 du modèle OSI (liaison de données).

Les ponts se basent sur l'adresse MAC (adresse en "dur" écrite dans l'interface) et le nom de la station sur le réseau pour savoir si la trame doit traverser le pont ou non. En d'autres termes, les informations ne passeront le pont que si elles doivent aller d'un réseau à l'autre.

Comme les ponts fonctionnent sur les couches basses du réseau, ils sont utilisables à peu près avec tous les protocoles. Ils n'offrent cependant que la possibilité d'interconnecter des réseaux physiques, ce qui limite considérablement leur emploi.

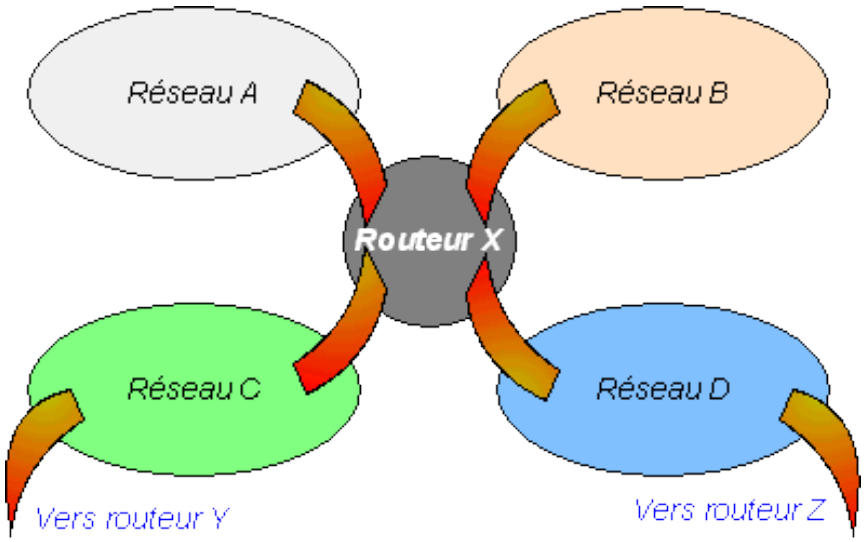
Les "switches", qui ressemblent à des "HUBs", fonctionnent sur ce principe. Alors qu'un "HUB" se contente de répéter toute information qui entre par l'un de ses ports sur tous les autres ports, un "switch" va mémoriser dans une table toutes les adresses MACS présentes sur chacun de ses ports et effectuera un pontage entre les ports concernés par un échange entre deux machines. Ce fonctionnement procure deux avantages :

- le trafic est mieux réparti sur le réseau, si l'architecture a été convenablement réalisée,
- l'espionnage du réseau par des "sniffeurs" devient largement limitée, sauf à utiliser des outils

spéciaux, plus facilement repérables par l'administrateur.

Les routeurs

Les routeurs sont plus puissants: ils sont capables d'interconnecter plusieurs réseaux utilisant le même protocole entre eux. Ils travaillent au niveau de la couche 3 du modèle OSI (couche réseau) et tous les protocoles n'utilisent pas cette couche. C'est pourquoi l'on parle de protocoles "routables" ou "non routables". NetBEUI n'est pas routable, TCP/IP et IPX/SPX le sont.



Les routeurs disposent d'une table de routage qui leur permet d'aiguiller les trames vers le bon réseau. Ils permettent une structure maillée, indispensable pour la construction de l'INTERNET.

De plus, les routeurs peuvent utiliser divers protocoles pour maintenir entre eux leurs tables de routage. Ils sont capables d'exploiter plusieurs routes possibles pour rejoindre la même cible, en choisissant la meilleure à un instant donné en fonction de critères simples (la moins chère, la plus rapide ou tout simplement celle qui marche). Ces fonctions sont indispensables sur les réseaux maillés qui permettent la tolérance de pannes sur les routes.

Les passerelles

Pris au sens large, une passerelle est un outil permettant de passer d'un réseau à un autre. Dans un réseau TCP/IP, l'adresse du routeur dans le réseau est dite "adresse de passerelle".

Au sens strict du terme, une passerelle est un outil permettant de faire communiquer entre eux deux réseaux n'utilisant pas le même protocole. La passerelle doit alors dépouiller la trame des informations spécifiques au protocole émetteur et les remplacer par leurs équivalentes dans le protocole récepteur!

Pour en savoir plus

Vous trouverez sur ce site quelques explications supplémentaires sur les points suivants:

- ROUTAGE pour mieux comprendre le fonctionnement du routage inter réseaux
- Le partage d'une connexion et Netfilter (Linux 2.4.x) pour apprendre à réaliser une passerelle entre son réseau domestique et un accès Internet, les deux chapitres sont complémentaires.

6- Le modèle OSI

La communication sur un réseau

Un peu de théorie...

Le fondement d'un bon réseau, c'est que le système d'exploitation soit capable:

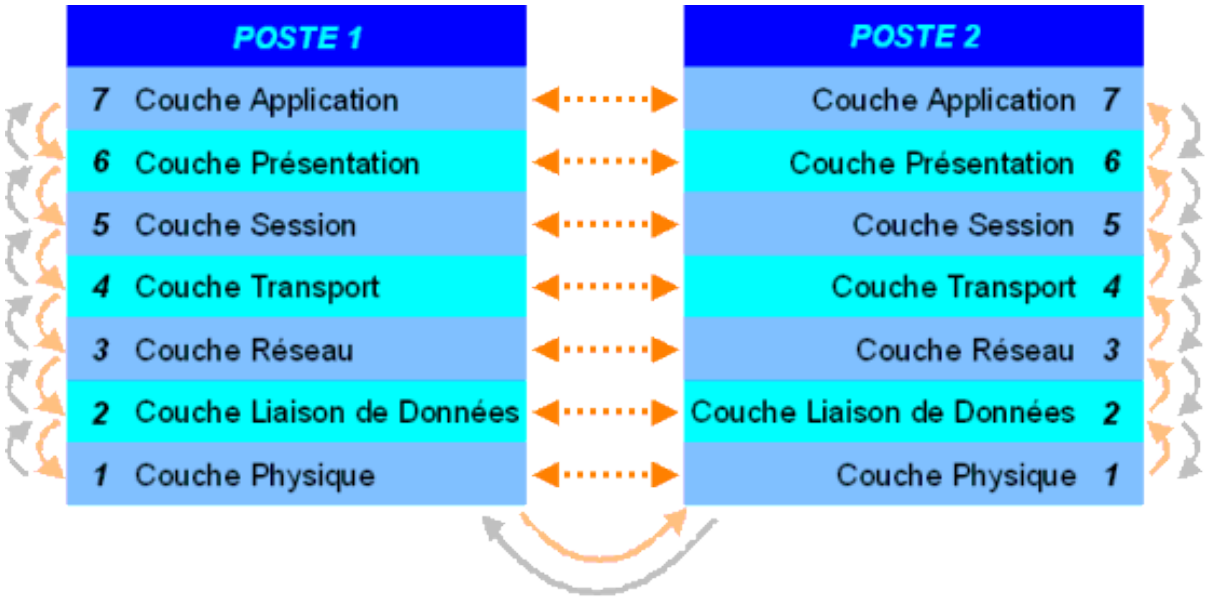
- De gérer la transmission de données.
- De fournir aux applications des interfaces standard pour leur permettre d'exploiter les ressources du réseau.

C'est le cas de tous les systèmes d'exploitation à jour.

A priori, rien ne devrait obliger les plates formes client et serveur à fonctionner avec le même système d'exploitation. C'était le cas pour les solutions propriétaires, c'est impensable aujourd'hui. Même si un réseau Microsoft dispose d'outils qui lui sont spécifiques, les hôtes de ce réseau peuvent tout de même dialoguer avec ceux d'un réseau Unix.

Pour arriver à cette interopérabilité, il faut que les divers protagonistes se mettent d'accord sur les fonctionnalités à implanter dans leurs applications et leurs fonctions réseau. C'est le rôle des RFC (Request For Comment) et des normes que de définir ces critères.

C'est l'objectif du modèle théorique O.S.I. qui décrit comment l'O.S. réseau, encore appelé N.O.S. doit être construit. Il décrit l'architecture en 7 couches logicielles présentant chacune des interfaces standard pour communiquer entre elles.



Considérations générales

Même si ce modèle reste très théorique, il a le mérite d'être le plus méthodique. (C'est d'ailleurs sa raison d'être).

Il y a deux points qu'il convient de bien comprendre avant tout:

- Chaque couche est conçue de manière à dialoguer avec son homologue, comme si une liaison virtuelle était établie directement entre elles.

- Chaque couche fournit des services clairement définis à la couche immédiatement supérieure, en s'appuyant sur ceux, plus rudimentaires, de la couche inférieure, lorsque celle-ci existe.

Description succincte des couches

La couche physique: 1

C'est la couche spécifique à la "tuyauterie" du réseau. Elle permet de transformer un signal binaire en un signal compatible avec le support choisi (cuivre, fibre optique, HF etc.) et réciproquement.

Cette couche fournit des outils de transmission de bits à la couche supérieure, qui les utilisera sans se préoccuper de la nature du médium utilisé.

La couche liaison: 2

Cette couche assure le contrôle de la transmission des données. Une trame doit être envoyée ou reçue en s'affranchissant d'éventuels parasites sur la ligne. Le contrôle est effectué au niveau du paquet de bits (trame), au moyen d'un "checksum".

Elle est elle-même divisée en deux sous-couches.

- La sous-couche MAC (Medium Access Control). C'est à ce niveau que l'on trouve le protocole de diffusion de l'information: Ethernet, Token Ring, ATM, etc. Pour un réseau domestique, c'est Ethernet qui est utilisé
- Par ailleurs, cette couche fournit des services de base pour la transmission de données, via LLC (Logical Link Control) ou HDLC (High level Data Link Control). Ces services peuvent être classés en trois groupes:
    - Les services sans connexion et sans acquittement.
    - Les services sans connexion, mais avec acquittement.
    - Les services orientés connexion.

Nous aurons l'occasion de reparler de ces notions plus loin, dans les protocoles UDP et TCP.

Cette couche fournit des outils de transmission de paquets de bits (trames) à la couche supérieure. Les transmissions sont "garanties" par des mécanismes de contrôle de validité.

La couche Réseau: 3

Cette couche assure la transmission des données sur les réseaux. C'est ici que la notion de routage intervient, permettant l'interconnexion de réseaux différents. C'est dans le cas de TCP/IP la couche Internet Protocol. En plus du routage, cette couche assure la gestion des congestions. Il faudrait beaucoup développer ce chapitre pour être clair. Disons simplement que lorsque les données arrivent sur un routeur, il ne faudrait pas que le flot entrant soit plus gros que le flot sortant maximum possible, sinon il y aurait congestion. Une solution consiste à contourner les points de congestion en empruntant d'autres routes (phénomène bien connu des vacanciers sur les routes).

Le problème de la congestion est un problème épineux, auquel il nous arrive assez souvent hélas d'être confrontés.

Cette couche est la plus haute dans la partie purement "réseau".

Cette couche fournit des outils de transmission de paquets de bits (trames) à la couche supérieure. Les transmissions sont routées et la congestion est contrôlée.

La couche Transport: 4

Cette couche apparaît comme un superviseur de la couche Réseau. Qu'est-ce à dire? Il n'est par exemple pas du ressort de la couche réseau de prendre des initiatives si une connexion est interrompue. C'est la couche Transport qui va décider de réinitialiser la connexion et de reprendre le transfert des données.

Son rôle principal est donc de fournir à la couche supérieure des outils de transport de données efficaces et fiables.

La couche Session: 5

La notion de session est assez proche de celle de connexion. Il existe cependant quelques détails qui peuvent justifier la présence de ces deux concepts.

Une seule session peut ouvrir et fermer plusieurs connexions, de même que plusieurs sessions peuvent se succéder sur la même connexion. Comme cette explication n'est pas forcément claire pour tout le monde, essayons de prendre quelques exemples:

- Vous avez un message à transmettre par téléphone à un de vos amis, votre épouse doit faire de même avec celle de ce même ami.
  Vous appelez votre ami (ouverture d'une connexion), vous discutez avec lui un certain temps (ouverture d'une session), puis vous lui dites que votre épouse voudrait parler à la sienne (fermeture de la session).
  Les épouses discutent un autre certain temps (ouverture d'une seconde session), puis n'ont plus rien à se dire (fermeture de la seconde session) et raccrochent (fin de la connexion).
  Dans cet exemple, deux sessions ont eu lieu sur la même connexion.
- Vous avez un travail à réaliser avec un collègue, par téléphone. Vous l'appelez (ouverture de la connexion et ouverture de la session). Il vous demande des informations qui nécessitent de votre part une recherche un peu longue, vous raccrochez après lui avoir dit que vous le rappellerez ultérieurement (fermeture de la connexion, mais pas de la session).
  Votre recherche effectuée, vous rappelez votre collègue (ouverture d'une seconde connexion pour la même session), vous lui transmettez les informations demandées, vous n'avez plus rien à vous dire (fermeture de la session), vous raccrochez (fermeture de la connexion).
  Dans cet exemple une session s'étend sur deux connexions.

Cette couche fournit donc à la couche supérieure des outils plus souples que ceux de la couche transport pour la communication d'informations, en introduisant la notion de session.

La couche Présentation: 6

Cette couche est un peu un "fourre tout" de la conversion entre représentation interne et externe des données. Là encore, cette explication n'est pas d'une grande clarté... Prenons donc quelques exemples.

Le format de codage interne des données

Les "mots" sont une suite d'octets. Un mot de 32 bits est donc une collection de 4 octets. Chez Intel, les octets sont numérotés de droite à gauche, alors que chez Motorola, ils le sont de gauche à droite. Il s'en suit que si une machine à base Intel envoie des mots à une machine à base Motorola, il vaut mieux tenir compte de ce détail pour ne pas s'y perdre...

D'autres exemples pourraient être trouvés dans le style, comme la complémentation à 1 ou à 2 pour les représentations négatives, les divers dialectes ASCII etc.

La compression des données.

Certains transferts de données se font par le biais d'algorithmes de compression. C'est intéressant pour certains types de documents comme le son, l'image ou la vidéo. Dans le modèle OSI, ces algorithmes sont fournis par la couche présentation.

Le cryptage des données.

Même chose pour la cryptographie.

Ce ne sont que des exemples, le modèle définissant bien d'autres fonctions.

La couche Application: 7

A priori, cette couche pourrait être la plus simple à comprendre, ce n'est pas obligatoirement le cas. En effet, dans le modèle OSI, cette couche propose également des services: Principalement des services de transfert de fichiers, (FTP), de messagerie (SMTP) de documentation hypertexte (HTTP) etc.

Dans le modèle, les applications ayant à faire du transfert de fichiers utilisent le service FTP fourni par la couche 7.

Ce modèle théorique, extrêmement détaillé est fait pour que chaque couche puisse être construite indépendamment des couches qui sont immédiatement au dessus et au dessous d'elle.

Un peu plus de pratique

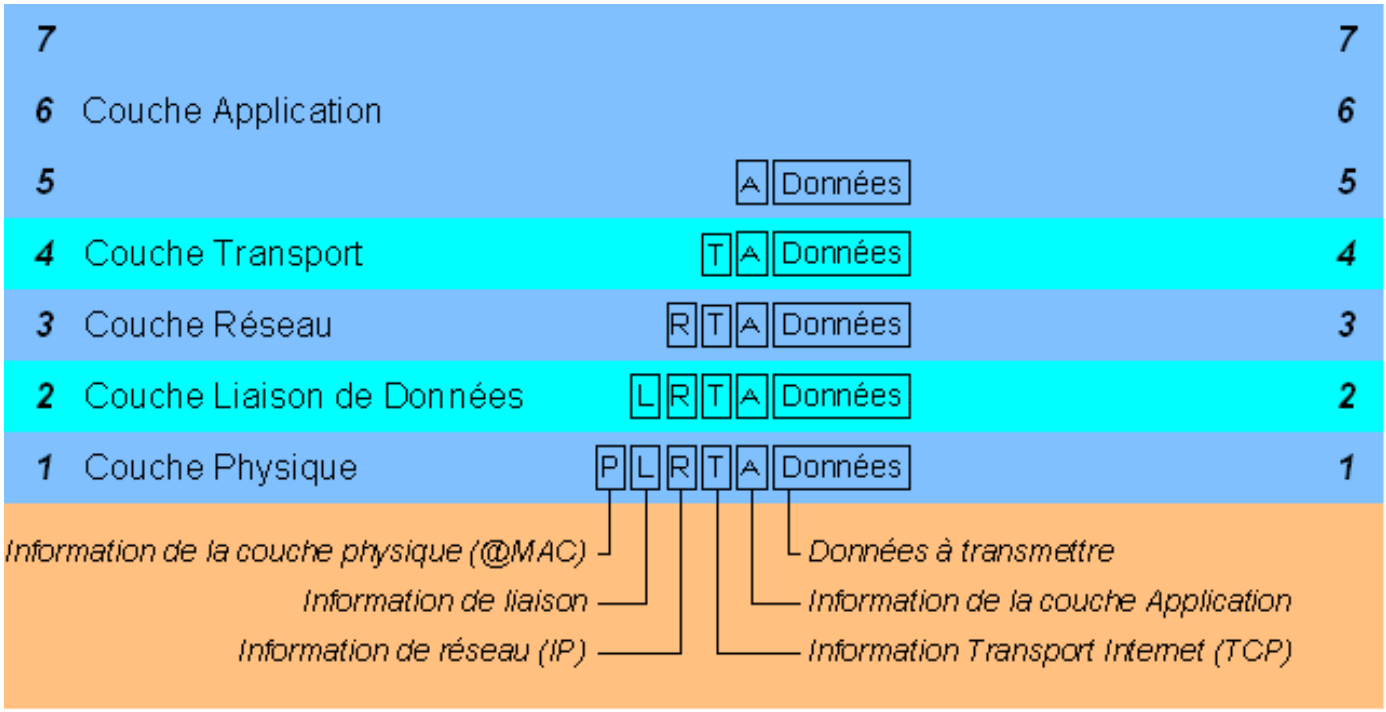
Modèle OSI	Modèle DOD
7 Couche Application	Couche Application
6 Couche Présentation	
5 Couche Session	
4 Couche Transport	Couche Hôte à Hôte
3 Couche Réseau	Couche Internet
2 Couche Liaison de Données	Couche Accès Réseau
1 Couche Physique	

Le modèle O.S.I. est tellement théorique qu'il va à l'encontre de l'efficacité. Il est donc souvent simplifié. Les simplifications se bornant toutefois à regrouper les fonctions de plusieurs couches O.S.I. en une seule. Exemple: Le modèle D.O.D. utilisé dans le protocole TCP/IP.

Cependant, les couches O.S.I. restent une référence dès lors que l'on parle de transmission de

données sur un réseau.

Lorsqu'une information (Données) est émise par une application, cette donnée descend les diverses couches du réseau, en récupérant au passage des informations supplémentaires à chaque couche, comme le montre l'illustration suivante.



Les trames qui circulent sur le réseau contiennent donc non seulement les données des applications, mais également tout un tas d'informations rajoutées par le N.O.S. Ces diverses informations permettront entre autres fonctions:

- Le pontage
- Le routage
- L'identification du poste émetteur
- L'identification du poste récepteur
- L'identification de l'application Emettrice
- L'identification de l'application Réceptrice.

Lorsque la trame entre dans le récepteur, elle remonte les couches qui lui enlèvent au passage les informations qui les concernent, si bien que l'application reçoit ses données sans se préoccuper de la façon dont elles ont été transportées.