

Communication Réseau

Lorsque deux ordinateurs veulent communiquer, il ne suffit pas de trouver un câble pour les relier entre-eux, car bien que cette possibilité existe dans Windows (communication directe par câble), ce n'est pas praticable dans un environnement de travail normal d'entreprise.

Pour en finir avec la communication directe par câble, on peut trouver cette option dans le menu du même nom de Windows ou l'installer comme accessoire s'il n'y figure pas. Ceci fait, on aura la possibilité au moyen d'un câble spécial « nul modem » (ressemble à un câble d'imprimante) de connecter deux ports Parallèles ou série et par ce moyen d'avoir accès aux fichiers partagés d'une machine à partir de l'autre et vice et versa.

Les réseaux dont nous allons parler sont un tant soit peu plus compliqués mais visent le même but : partager des ressources (imprimante, disques de serveur, CD-Rom) entre plusieurs utilisateurs.

Réseaux

Bien que l'on ait de multiples choix et de nombreuses normes pour les réseaux, on trouve la plupart du temps dans les entreprises des réseaux ethernet avec connecteur RJ45 (voir carte).

Ces réseaux sont du type étoile, c'est à dire que chacune des machines est au bout d'un fil et que l'autre bout est relié à un concentrateur, un nœud qui peut être de type hub ou switch.

A noter que les connecteurs BNC (coaxiaux, « thin ethernet ») en voie de disparition étaient de type « brin » de sorte que plusieurs machines étaient branchées via un T sur un câble (longueur maximum 180m) avant d'arriver sur un concentrateur. Ces câbles étaient obligatoirement terminés par une résistance coaxiale de 50 ohm (nom : 10 base 2).

Voici un exemple de carte réseau avec un connecteur RJ45. Le protocole supporté par cette carte est 10/100 base TX que l'on peut décomposer en « 10Mbits/100Mbits avec connecteur RJ 45 » La norme gigabit 10/100/1000 équipe de plus en plus de cartes, mais les câbles doivent également supporter ce débit.

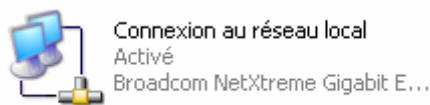


La norme des câbles est UTP 5 pour le trafic à 100Mb/s UTP 7 pour le 1Gb/s. La norme définit une atténuation par mètre de longueur. Ainsi, un câble UTP7 pourra fonctionner correctement avec du trafic 100Mb/s sur une plus grande longueur que un UTP5 (200m)

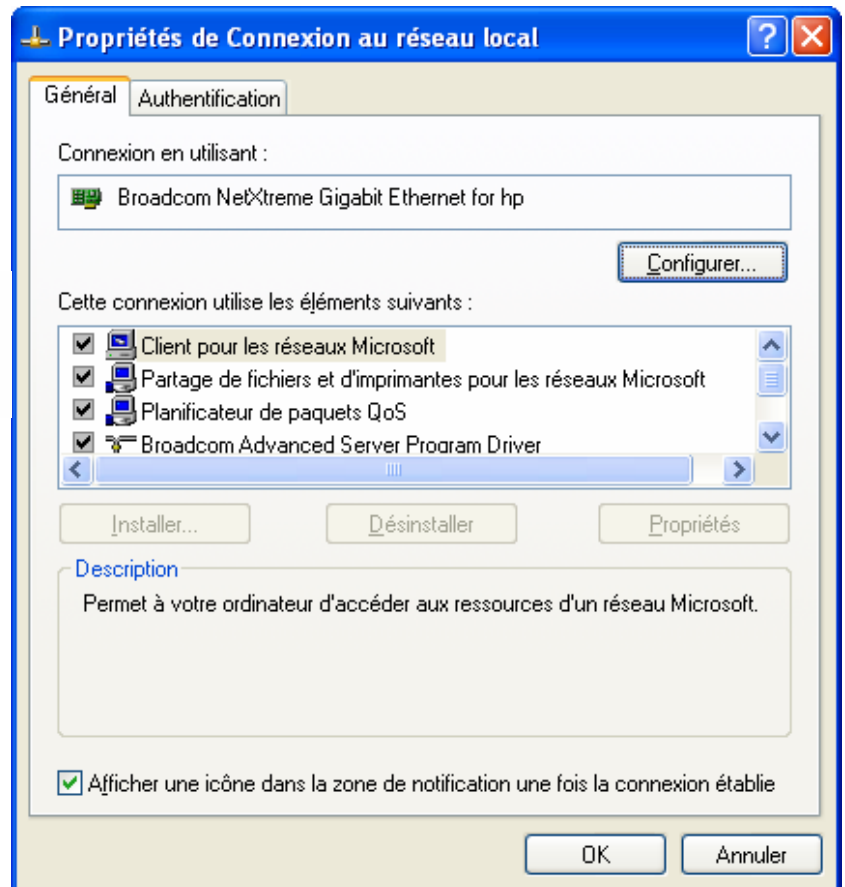
Ethernet, TCP/IP

Ce sont les protocoles généralement utilisés pour la communication entre machines à l'intérieur des entreprises. On fait aujourd'hui passer de la voix sur IP (téléphone) et de la vidéo, on l'utilise à toutes les sauces y compris comme bus de terrain pour la communication entre capteurs et unités de traitement.

Une carte réseau s'installe en principe toute seule. On trouve généralement le driver dans windows, mais parfois, il est dans le carton avec la carte ou sur internet chez le fabricant.



Pour configurer manuellement une carte, ouvrir les connexions réseau dans le panneau de configuration. Et après avoir choisi la connexion en question, l'on tombe sur la fenêtre ci-contre. Chaque ligne des « éléments » de cette configuration se rapporte à un protocole ou un service utilisé par windows.



Partage :

Le dernier point sera le clic sur « partage et sécurité » que l'on trouve en faisant un clic droit sur un répertoire (ou une imprimante) de la machine serveur

A noter que windows XP installé par défaut vous propose le minimum vital pour le partage de documents, qui ne comprend pas de gestion de droits. (partagé ou non partagé)
Cela nous ramène à l'air windows 98 où il n'était pas possible de protéger une machine.

Cet art difficile de la gestion de droits d'accès peut conduire à ne plus avoir accès à ses propres fichiers mais permet également de définir sur sa machine un répertoire que tout le monde peut accéder en lecture sans partager à tous vents le reste du disque.

Pour activer la gestion de droits étendue (pour moi, normale) il faut chercher la petite croix dans les options des dossiers « utiliser le partage de fichiers simple » et l'enlever.

Cette gestion des droits « avancée » permet pour chaque dossier ou même chaque fichier de déterminer qui peut :

- Le modifier
- Le lire et exécuter
- Afficher le contenu des dossiers
- Lire seulement
- Ecrire seulement
- Avoir le contrôle total.

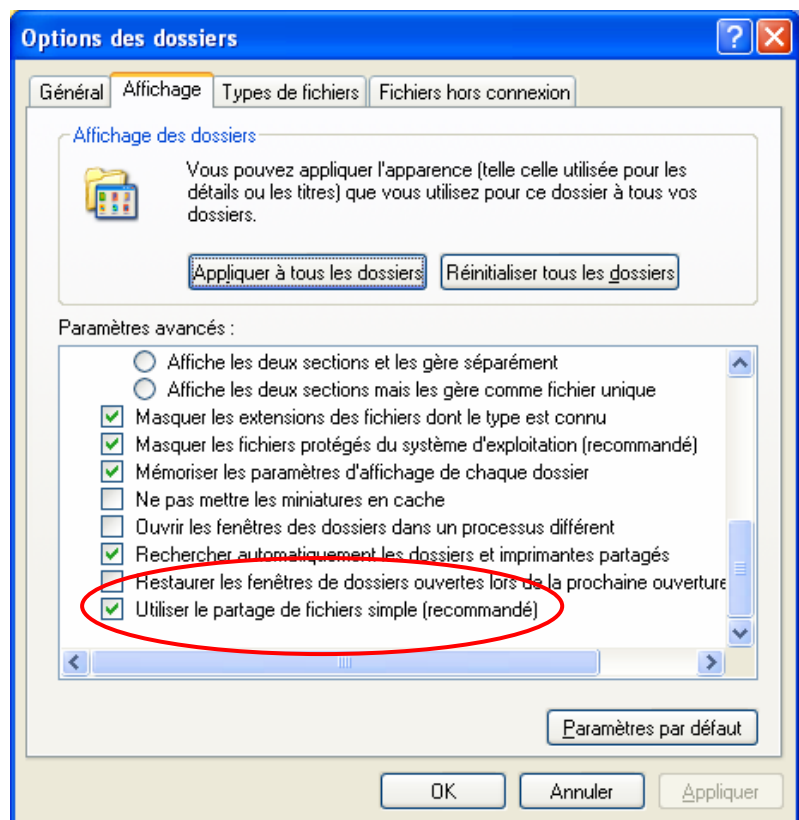
Chaque utilisateur ou groupe d'utilisateur pourra ainsi avoir des droits différents.

Les administrateurs ont par principe des droits étendus mais surtout, la permission de les changer.

Toujours s'assurer d'avoir un compte administrateur disponible avant de changer les droits d'accès.

Attention : il n'y a pas d'autorisation mais que des restriction, ce qui veut dire que si l'on interdit à « tout le monde » de lire tel répertoire, un administrateur qui aurait des droits de lecture spécifiés explicitement ne pourrait pas les exercer car une interdiction a toujours la priorité sur une autorisation.

Indiquer avant de sortir de la gestion des droits si on veut appliquer ces restrictions à tous les fichiers ou répertoires enfants du répertoire courant (logiquement oui.).



Adressage IP

On ne détermine pas n'importe comment le « range » d'adresse que l'on va attribuer à un réseau. Chaque taille de réseau aura sa classe d'adresse (A,B,C) qui va déterminer les adresses utilisables.

Je rappelle ici que toute adresse IP se décompose en adresse de réseau et adresse de machine.

Exemple pour l'adresse précédente de classe A : 10.10.10.10 masque 255.0.0.0 nous avons les informations suivantes :

Réseau 10.10.10.10 Machine

Nous allons observer maintenant les définitions des différentes classes d'adresses :

Classe A

Pour les grands réseaux, masque 255.0.0.0

On pourra placer sur chacun de ces réseaux 256x256x253 soit 16'580'608 machines différentes.

Le dernier octet n'est pas utilisable comme numéro de machine pour ses valeurs 0 et 255, ces deux numéros étant respectivement l'adresse de réseau et l'adresse de demande d'identification (« Eh ! , oh !, y a quelqun ? ») ou « adresse de broadcast ».

Les adresses de classe A commencent toujours par un « 0 » binaire dans le premier octet, ce qui définit les adresses 1.0.0.0 à 126.0.0.0 soit 126 réseaux différents.

Classe B

Pour les réseaux de moyenne grandeur, masque : 255.255.0.0

On pourra placer sur chacun de ces réseaux 64768 machines soit les adresses de machines 0.1 à 255.254 les adresses 0 et 255 étant toujours respectivement les numéros de réseau et de broadcast

Les adresses de réseau utilisables dans ce cas doivent commencer par un « 10 » binaire, soit des numéros de réseau de 128.1.0.0 à 191.254.0.0 nombre de réseaux : 16382.

Classe C :

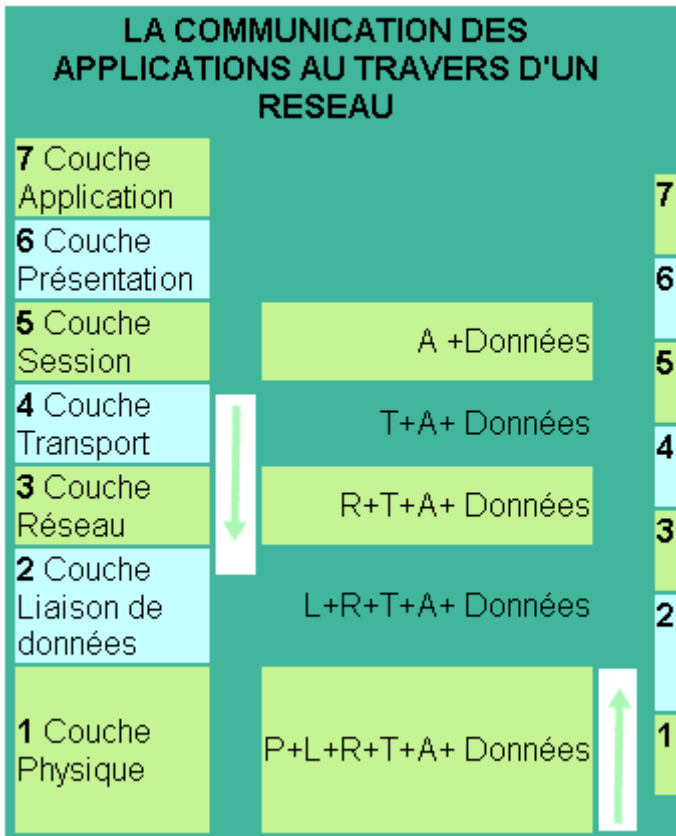
Pour les petits réseaux, masque de sous réseau : 255.255.255.0

Les adresses machines que l'on pourra utiliser ensuite seront par groupe de 253, le 0 étant le numéro de réseau et le 255 broadcast.

Les adresses de réseau utilisables doivent commencer par un « 110 » binaire dans le premier octet, soit les adresses de réseau 192.0.1.0 à 223.255.254.0 ce qui représente le nombre respectable de 2097152 de réseaux différents.

Parmi ces classes d'adresse, trois ranges ont été définis pour l'utilisation privée en entreprise, ces adresses sont typique de réseau internes et ne sont pas « routables », ce qui veut dire que le moindre paquet qui s'aventure sur internet avec une de ces adresses comme source ou destination sera immédiatement mis à la poubelle par le premier routeur qu'il croisera.

Ces ranges sont :
Classe A : un seul réseau, 10.0.0.0
Classe B : 172.16.0.0 à 172.31.0.0
Classe C : 192.168.0.0 à 192.168.255.0



Modèle de communication

Pour établir une communication, il faut se mettre d'accord au préalable sur un certain nombre de choses, et on a catégorisé en un modèle en 7 couches (layers) les différentes étapes de la communication. Ce modèle porte le doux nom de modèle OSI.

Nous allons le parcourir de haut en bas, puis de bas en haut, ce qui est le trajet normal du parcours de l'information d'une machine vers l'autre. D'une application vers une autre application en passant par toutes les étapes d'une transmission qui va traiter des différentes problématiques étape par étape (couche par couche).

Couche N° 7 : **Application**

Cette couche est la couche visible pour l'utilisateur, c'est le browser internet ou l'explorateur de fichier. C'est de là que tout commence et là que tout abouti.

Couche N°6 : **Présentation**

Couche de mise en forme, de traduction des lettres en code machine, de compression ou de cryptage des données.

Couche N°5 : **Session**

Couche chargée de maintenir la communication entre les machines, de décider qui parle et par exemple si la communication est en half-duplex (chacun parle à son tour) ou en full-duplex (les deux peuvent émettre en même temps).

Couche N°4 : **Transport**

Elle se charge de la protection des données, les subdivise en segments, génère des tests pour contrôler la validité des données et leur intégrité après le transfert.

Couche N°3 : **Réseau**

Cette couche choisi une route pour le message, elle organise les segments en paquets, les compte, et ajoute un entête indiquant l'enchaînement des paquets et l'adresse de l'ordinateur destinataire.

Couche N°2 : **Liaison**

Supervise le transport des données elle confirme la somme de contrôle et garde une copie des paquets jusqu'à la confirmation de bonne réception du point suivant de la route.

Couche N°1 : **Physique**

Traduit les paquets suivant le support de transmission (analogique, hertzien, ...)





Connexion

On trouve sur les réseaux quantité d'appareils nécessaires à la bonne communication entre ses membres, en voici une description succincte

Répéteur ou hub :

Petite boîte qui compte un certain nombre de prises RJ45 (4 à 24) et qui relie plusieurs stations entre-elles. C'est un appareil de couche 1, il ne fait que répéter les signaux qui lui parviennent sur tous les ports qu'il possède. C'est le dernier nœud de la structure en étoile des réseaux.



Switch :

Le switch est un répéteur un peu spécial qui ne va répéter le signal provenant d'un poste que sur le brin où il sait se trouver le poste cible du message. Il tient donc à jour toutes les adresses des cartes réseau qui envoient des paquets sur ses brins. Ce mode de fonctionnement permet de limiter les collisions entre paquets lorsque deux machines commencent à « parler » en même temps. Et donc d'accélérer le débit des connections lorsque le nombre de machines devient élevé.



Le switch intervient au niveau de la couche de liaison 2, il faut toujours un peu de temps à un switch pour qu'il s'aperçoive qu'une machine est passée d'un brin à un autre.

Ce temps de latence de quelques minutes pour un switch tout seul peut passer à 30 minutes pour un réseau quelque-peu compliqué. On comprend pourquoi certains réseaux d'entreprise mettent tellement de temps à retrouver leurs esprits.

Routeur

Nous avons vu que les réseaux sont définis par leur masque de sous réseau (255.255.255.0 p.ex) et que deux machines doivent impérativement se trouver sur le même réseau pour communiquer ensemble.

Il n'en demeure pas moins qu'il est parfois utile de sortir de son LAN (Local Area Network) pour explorer le vaste monde et par conséquent, il est nécessaire de connecter des réseaux différents. C'est là le travail du routeur.

Le routeur est configuré pour aiguiller les paquets vers le réseau de destination, il comporte donc une table de routage qui lui indique que le réseau 10.10.10.0 mask 255.255.255.0 est situé sur son interface (carte réseau) 1 et que le réseau 172.16.0.0 mask 255.255.0.0 est sur l'interface 2

Pour tous les paquets dont il ignore sur quelle patte il doit les envoyer, le routeur dispose d'une adresse par défaut (chemin vers internet) ou il envoie tous les paquets inconnus.

Le routeur est un appareil de niveau 3, réseau.

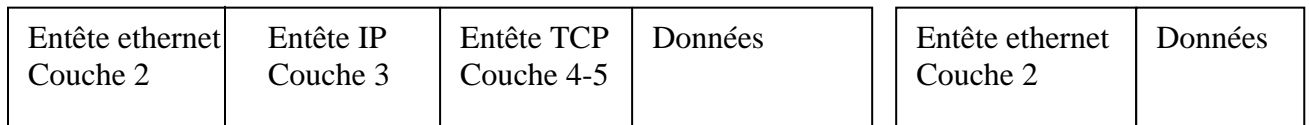


Paquet TCP/IP

Pour comprendre la nature des communications entre deux entités, nous avons vu les différentes couches du modèle OSI, mais il est intéressant d'observer un résultat concret de cette théorie. Les protocoles sont ce qui définit la manière de se parler et chacun a son rôle dans la nébuleuse internet.

Nous allons disséquer pour cela un paquet TCP/IP circulant sur un réseau ethernet.

Sens de lecture des paquets →



Et voici en détail la composition des entêtes de ces différents protocoles.

Entête ethernet :

12 bytes Adresse de destination	12 bytes Adresse source	4 bytes Longueur
------------------------------------	----------------------------	---------------------

La longueur d'un paquet ethernet est au maximum de 1500 bytes.

Les deux adresses en question sont les MAC adresses (Media Access Control) Ces adresses sont celles des cartes réseau.

Entête IP :

4 bits version	4 bits long. Entête	8 bits Type Of Service	16 bits longueur totale	
16 bits identification		3 bits flags	13 bits fragment offset	
8 bits Time To Live	8 bits Protocole	16 bits checksum d'entête		
32 bits adresse IP source				
32 bits adresse IP destination				
Options				

Les premiers champs sont relativement clairs, sauf peut-être Type Of Service (TOS) qui permet de marquer des paquets pour indiquer la manière de les traiter (« urgent, liaison ne souffrant pas de délais (téléphone)» ou « tranquille, c'est de l'http, on a le temps »)

Vient ensuite le champ Time To Live (TTL) qui donne une durée de vie au paquet et évite ainsi que des paquets envoyés il y a deux mois tournent encore dans le réseau en peine d'adresse cible. Les deux champs d'adresse source et cible sont ceux qui contiendront les adresses IP de la machine émettrice et réceptrice du paquet.



Entête TCP :

16 bits Port source								16 bits Port destination	
32 bits Numéro de séquence									
32 bits Numéro de confirmation									
4 bits lg. Entête	7 bits réserve	URG	ACK	PSH	SYN	FIN	16 bits Taille de la fenêtre		
16 bits validation								16 bits degré d'urgence	
Options									

L'entête TCP (couche de session) va contenir les informations de connexion entre les machines : quel port parle, quel port écoute, de quelle session il s'agit, ...

Les ports en question sont les ports logiques de la machine. Ils sont au nombre de 65535 et permettent une communication HTTP (port cible 80) en même temps qu'une communication SMTP (port cible 25) sans que les paquets ne se mélangent.

A noter que le serveur écoute toujours sur le même port (< 1024) et que les clients vont changer leur port source pour éviter que deux clients parlent au serveur du même port (>1024).

On peut d'ailleurs reconnaître un serveur WEB sur le réseau car il va écouter sur son port 80 et répondre à tout paquet adressé à celui-ci (par exemple en le sollicitant par un essai d'ouverture de session telnet sur ce port).

Restent les numéros de séquence et de confirmation qui sont là pour valider la continuité de la session et qui seront modifié selon une règle fixe à chaque paquet. D'où une difficulté de détourner une session sur la machine d'un tiers (hacker) car il faut reprendre la conversation à ou elle en était sans quoi la session va être coupée.

Suite TCP/IP:

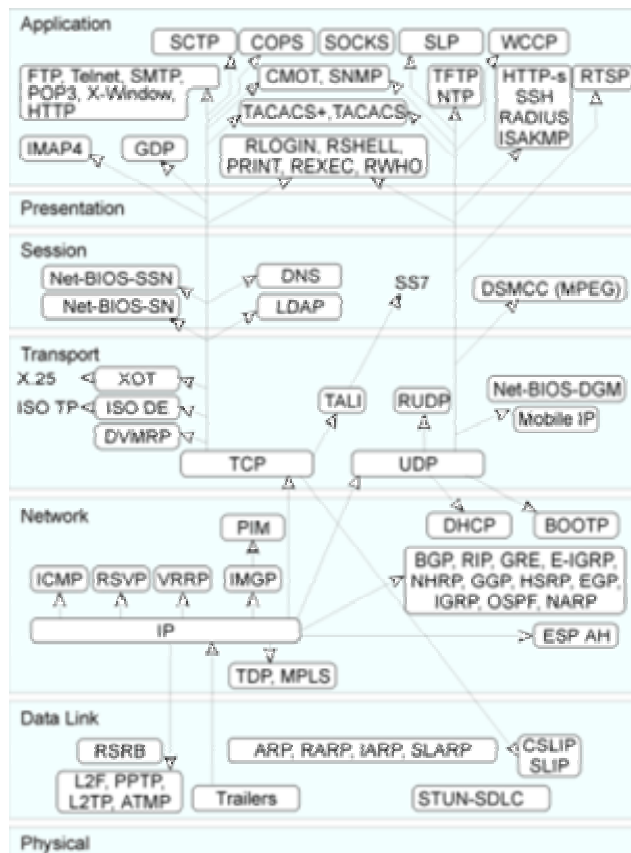
Pour vous donner une idée de la diversité des protocoles existants, voici un aperçu de la suite de protocoles attachés à TCP/IP.

Il semble que l'on a énormément de protocoles différents, mais ce n'est qu'une petite partie de ce que l'on trouve en télécommunication.

TCP/IP est destiné à des réseaux LAN (Local Area Network), aire dans laquelle on trouve également d'autres protocoles (Appletalk, Token Ring, FDDI, ...)

Mais si l'on regarde du côté du WAN (Wide Area Network) on retrouve au moins autant, voir largement plus de protocoles différents pour le transport des paquets.

Je ne citerai que Framerelay ou ATM comme exemple qui ont chacun un chapelet de protocoles associés.



Pour plus de détail sur un des animaux de la jungle des protocoles, on trouve les spécifications de chacun d'eux sur la toile.