

NOTIONS SOMMAIRES sur les RESEAUX

Présentation

Un **réseau** est constitué de machines connectées entre elles et capables d'échanger des données, des fichiers, des programmes.

Dans un réseau **poste à poste** toutes les machines ont la même importance et l'échange d'informations se fait sans réel contrôle.

Le "**poste à poste**" ne se pratique que pour de petits réseaux locaux (LAN Local Area Network).

WINDOWS 98 et XP Vista et Seven permettent de connecter rapidement plusieurs machines sur ce modèle (par exemple celles d'une salle de classe de lycée).

En général les réseaux informatiques sont du type **client-serveur**.

L'ordinateur-**serveur** met à disposition ses informations et l'ordinateur-**client** en dispose.

Le **serveur** est la pièce maîtresse du réseau et le **client** peut parfois se réduire à une simple console (écran-clavier) sans disque dur ni lecteur de disquettes.

On distingue plusieurs types de serveurs :

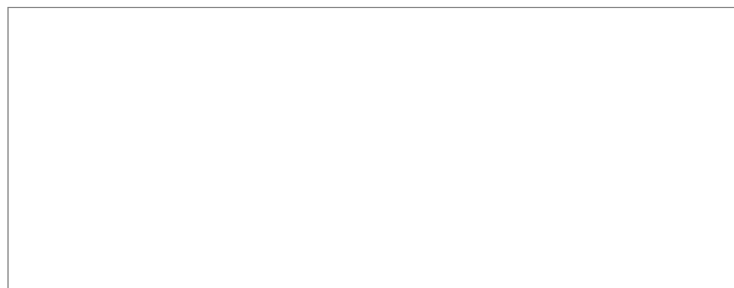
- Les **serveurs de fichiers** qui mettent des documents à disposition sur le réseau
- Les **serveurs d'applications** qui mettent des programmes sur le réseau, les **serveurs d'accès** qui contrôlent les accès au réseau (LOGIN) et les sorties (LOGOUT).
- Les **serveurs d'impression** qui mettent une imprimante à disposition de plusieurs clients,...

Un serveur peut remplir plusieurs fonctions, mais ce sont ses fonctions de contrôleur qui le distingue le plus. Il peut autoriser ou interdire l'accès à une **ressource** quelconque (fichier, programme, imprimante, autre réseau ou sous réseau,...).

Topologie d'un réseau :

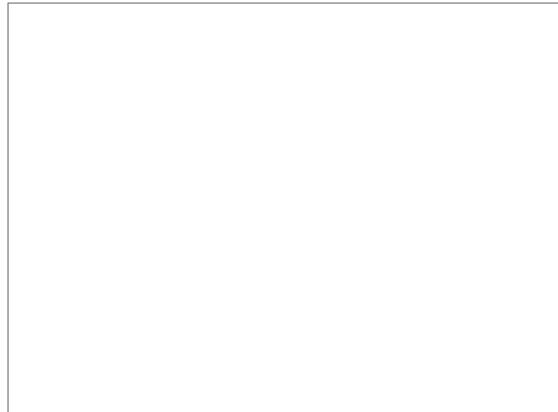
Les deux installations les plus classiques pour des petits réseaux sont décrites ci-dessous.

Les réseaux **poste à poste** ont en général une structure linéaire en **bus**.



Les machines sont reliées par un câble coaxial, les unes après les autres. Ce câble est muni d'une terminaison à chacune de ses extrémités pour éviter les réflexions parasites des signaux. Les deux inconvénients de cette architecture sont le débit limité à 10 Mbits/s et la possibilité de collision des **paquets** d'informations qui transitent sur le câble.

Plus performante est la **structure en étoile** avec un concentrateur électronique ("**hub**") au centre de l'étoile.



Le câble, le plus souvent blindé, qui relie les machines au **hub** comporte en général 4 paires de fils torsadés et se termine par des connecteurs RJ45.

Le débit standard actuel pour cette structure est de 100 Mbits/s (voire 1 Gbits/s). Les **hubs** peuvent être connectés entre eux et plusieurs serveurs peuvent cohabiter sur le même réseau, dans des segments différents. Cette topologie facilite donc une évolution hiérarchisée du matériel dans une même entreprise.

On désigne par LAN des réseaux dont l'étendue géographique reste limitée (quoique certains LAN peuvent comporter des centaines de machines).

Les WAN (Wide Area Network) peuvent eux être très étendus. Les câbles les plus longs sont en fibre optique et des connexions par **accès à distance** ("dial up") sont fréquemment utilisées (lignes téléphoniques ou spécialisées).

Protocoles réseaux

Pour que les machines puissent communiquer, elles doivent disposer d'une carte réseau (logée dans un connecteur interne). La carte réseau est reliée à une autre carte réseau ou à un hub avec un câble adéquat (suivant la topologie utilisée).

La communication du matériel se fait forcément suivant des règles de dialogue, c'est ce qu'on appelle le **protocole réseau**.

Les protocoles les plus utilisés sont : IPX/SPX, NETBEUI et **TCP/IP**.

Systèmes d'exploitation réseaux

Un OS (Operating System) peut se définir comme l'ensemble des programmes nécessaires à la gestion d'un ordinateur. Ce logiciel permet à l'utilisateur et aux autres logiciels d'exploiter les ressources matérielles de la machine et les divers périphériques installés (écran, clavier, souris, disques,...).

MS-DOS (de Microsoft) est un exemple très connu pour monopostes.

En réseau, un système d'exploitation particulier doit être utilisé pour pouvoir gérer le matériel réseau (cartes et hubs) et utiliser le protocole réseau. Voici rapidement quelques exemples :

Système d'exploitation	protocole associé
système UNIX	TCP/IP

NETWARE (de Novell)	IPX/SPX et TCP/IP
WINDOWS NT (de Microsoft)	NETBEUI, TCP/IP et IPX/SPX
Windows XP, vista, Seven (réseaux poste à poste)	NETBEUI, TCP/IP et IPX/SPX

Domaine

Dans le jargon-réseau, le mot **domaine** désigne un ensemble de **ressources** informatiques (matérielles ou logicielles) contrôlées par un **serveur**.

On parle aussi de sous domaines contrôlés par un serveur secondaire.

PRESENTATION rapide d'INTERNET

Que signifie Internet ?

L'étymologie est la suivante : **INTER** (relations, échange en Latin) et **Network** (réseau en Anglais) ;

La réalité est bien conforme à l'étymologie puisqu'Internet est effectivement une interconnexion de réseaux informatiques à travers le monde qui permet des échanges d'informations **multimédia** (textes, sons, images, vidéo, données numériques) rapides et au moindre coût.

Internet est donc un super W.A.N.

Naissance d'INTERNET

C'est en 1964, en pleine guerre froide, que le Ministère de la Défense des Etats-Unis réalise la connexion de ses réseaux de communications avec d'autres réseaux radio et satellites ; le but de ce projet NET était de toujours être capable de communiquer même en cas de destruction d'un réseau important. ARPANET est repris en 1969 pour relier plusieurs universités américaines et en 1972 une quarantaine de serveurs (NASA, MIT, UCLA,...) sont reliés en différents points des Etats-Unis. En 1993, le C.E.R.N. (Centre Européen de Recherche Nucléaires) développe des applications **multimédia** sur des réseaux déjà connectés : c'est la naissance du **World Wide Web**.

En 2000, Internet c'était quelque 50 millions de machines connectées

Le protocole de base

TCP/IP doit être installé sur toute machine connectée à l'internet. Son rôle se résume à faire communiquer les machines. Ce protocole doit son succès à :

- la possibilité de fonctionner avec n'importe quel système d'exploitation (Windows, Unix, McIntosh,...)
- sa versatilité **client-serveur**, la même machine pouvant à la fois être un serveur (mettre des informations à disposition) ou un client (lire des informations sur d'autres serveurs)
- la possibilité d'interconnecter **dynamiquement** les réseaux ;

IP (Internet Protocole) est la partie qui assure le cheminement de l'information de **nœuds** en nœuds (de **serveurs** en serveurs).

Toute machine connectée est repérée par une **adresse IP** codée sur 4 octets ("o1.o2.o3.o4"), il est donc théoriquement possible de connecter quelque quatre milliards de machines sur Internet ! ($2^{32} = 4\,294\,967\,296$)

TCP (Transmission Control Protocole) est la partie qui scinde les informations en **paquets** à l'expédition et les regroupe à destination TCP contrôle aussi l'intégrité des données et gère les erreurs de transmission.

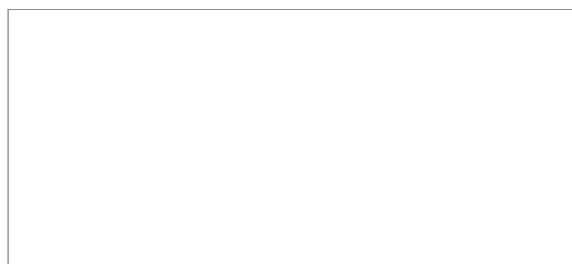
Quand on lit une page web située sur un serveur web à l'autre bout du monde, les paquets peuvent très bien transiter par des chemins différents. Si la page lue se trouve physiquement de l'autre côté de la rue, les paquets peuvent très bien faire le tour du monde avant d'arriver.

Les services ou protocoles annexes

Internet est un ensemble de **services** (pages multimédia, courrier, discussions, etc...) ; chaque service utilise un **protocole annexe** pour fonctionner.

Des **logiciels spécifiques** (explorer,.....) sont nécessaires pour utiliser ces services. Quand on installe sur une machine un de ces logiciels spécifiques, il installe automatiquement, par-dessus le protocole réseau TCP/IP, le protocole annexe adéquat.

On peut schématiser la configuration d'une machine "connectable" par un empilement de couches, la plus basse étant celle qui représente le matériel



Il existe maintenant de très nombreux protocoles logiciels (annexes) ; seuls les plus importants sont ici cités.

http (HyperText Transfert Protocole) est le protocole du **W.W.W.**(web) ; il permet de naviguer ("surfer") d'une page multimédia à une autre par l'intermédiaire de **liens hypertextes** actifs.

Le lien, qui peut être du texte (souligné) ou une image, **pointe** vers une autre page sur le même serveur ou sur un autre.

FTP (File Transfert Protocole) est le protocole permettant de **transférer des fichiers** d'une machine à une autre. Un **client** peut copier un fichier à partir d'un dossier d'un **serveur** ("downstream") et inversement ("upstream").

SMTP (Simple Mail Transfert protocole) est le protocole permettant l'échange de **courrier électronique** ("e-mail")

POP (Post Office Protocole) est plus récent que SMTP. Il ne sert qu'à la **remise de courrier**, mais permet de gérer plusieurs adresses électroniques et de les conserver dans la même "boîte aux lettres" (BAL) sur un serveur en attendant l'appel d'un client pour vider cette BAL.

NNTP (Network Net Transfert Protocole) est le protocole pour les **NEWS** (discussions en ligne) qui permet l'échange de messages entre les serveurs abritant les **NewsGroups** (forums de discussions), chaque forum traitant d'un sujet bien ciblé.

IRC (Internet Relay Chat) est le protocole pour les "**chats**" (prononcer "tchatte" au singulier) qui sont aussi (comme les news) des discussions en ligne par l'intermédiaire du clavier, mais en temps réel ; les clients se connectent sur un serveur spécifique, font connaissance et bavardent.

TELNET (TELEphone et Net) est le protocole permettant de se connecter sur un serveur fonctionnant avec le système d'exploitation UNIX. C'est le plus ancien service encore utilisé sur le Net.

Hiérarchie et domaines

La clé pour se connecter à Internet, autrement dit pour établir un "socket" (une prise) sur le net, c'est donc l'**adresse I.P.** qui identifie chaque machine. C'est une organisation de professionnels, l'INTERNIC, qui attribue ces adresses. Elle possède des antennes dans tous les pays.

En France, cette organisation s'appelle AFNIC (www.nic.fr).

L'adresse I.P. est transformée en clair par un service particulier, le DNS (Domaine Name Système ou protocole d'assignation des noms de domaine) tout serveur connecté fait donc appel à le protocole pour que son adresse en clair soit comprise sur le Net.

Une même page Internet peut donc être appelée soit :

- Par son adresse www.monsite.free.fr
- Par son adresse IP <http://209.143.134.xxx/> par exemple

Au niveau de l'entreprise ou du particulier, le premier contact passe obligatoirement par un **prestataire de services** ("provider" au sens large). Les providers sont des professionnels d'Internet, tous affiliés à un **NIC** national et donc reconnus par l'INTERNIC.

Plusieurs cas de figures sont envisageables.

- **On veut consulter** le WWW, les forums, avoir une boîte à lettres, etc... : il faut signer un contrat avec un FAI ("provider" au sens strict) qui donnera un accès (limité ou non) à Internet, moyennant un abonnement, sous forme d'un **nom d'utilisateur** ("login") et d'un **mot de passe**. En fait, le fournisseur d'accès attribue, au moment de la connexion de l'internaute, **une des adresses IP** dont il dispose à cette date. Si on est connecté par câble, donc en permanence (accès direct), certains FAI peuvent "louer" une **adresse IP sortante fixe**, mais ce n'est pas le même tarif.
- **On veut mettre à disposition** sur Internet des ressources diverses (pages multimédia, logiciels, forums, e-business, etc...) : il faut demander à un prestataire un **nom de domaine** ; le prestataire contacte le NIC national ou l'INTERNIC, s'assure de la recevabilité de la demande et de la disponibilité du nom demandé. Le **nom de domaine** et son **adresse IP associée** sont alors enregistrés par un NIC qui perçoit une rémunération. Cette adresse est alors une adresse permanente **entrante**, qui pointera sur le **serveur web** (et le réseau interne qu'il contrôle) qui abrite les **ressources à partager** (Site). Il vaut mieux évidemment

que le **serveur web** soit connecté et consultable en permanence ; il peut se situer sur les lieux même de l'entreprise, ou chez un prestataire-hébergeur (**serveur web virtuel**) qui sera rémunéré pour le service.

- **"Consulte mon site !"** Tout internaute qui se respecte a réalisé et mis en ligne ses propres pages web multimédia. Pour mettre en ligne des pages multimédia standards ne nécessitant pas de programmation évoluée, le plus simple est de faire **héberger** ses pages **chez un prestataire**, qui peut aussi être le **fournisseur d'accès**. Beaucoup de **FAI** proposent 10 Mo d'espace pour des pages et 5 boîtes à lettres compris dans l'abonnement pour l'accès à Internet. Certains sites spécialisés offrent même un **hébergement gratuit** (mais limité en espace). Dans ce cas, le "site" sera inclus dans un sous-domaine du prestataire qui attribuera l'adresse IP qu'il veut et imposera le nom de son domaine dans l'adresse textuelle du site.

Les noms de domaine sont classés en catégories identifiables par les derniers caractères après le dernier point. Les spécialistes appellent ces catégories **"top level domains"** (domaines de plus haut niveau).

- Beaucoup de ces suffixes sont délivrés par l'INTERNIC et "s'achètent aux Etats-Unis" :
 - .com désigne des domaines à caractère commercial ;
 - .net , des entreprises professionnelles d'Internet, des réseaux et communications ;
 - .edu , des établissements d'enseignement et universitaires ;
 - .org , des associations et organismes à but non lucratif ;
 - .mil , des organismes militaires ;
 - .gov , des organismes gouvernementaux ; etc...
- Puis viennent les **"top level domains" nationaux**, délivrés par les NIC nationaux et qui rassemblent toute sortes de domaines établis dans un **pays** bien précis :
 - .fr (France), .be (Belgique), .nl (Pays-Bas), .de (Allemagne), .it (Italie), .sp (Espagne), .gr (Grèce), .uk (Royaume Uni), .ca (Canada), .us (Etats Unis), etc....

Les NIC contrôlent l'attribution des noms de domaine ; par exemple, un lycée public français ne peut pas prendre un domaine .fr puisqu'il est géré par une Académie. Il ne peut devenir que sous-domaine du domaine d'une Académie, ou se contenter d'un dossier de ce sous-domaine ; il ne peut pas prendre un .edu car cela est réservé aux établissements délivrant un diplôme BAC + 4.

Le protocole TCP/IP et internet

Introduction

TCP/IP est un ensemble de logiciels développés au fil des années (à partir des années 70 déjà) qui constituent un "langage universel" de communication informatique à travers le monde. Le protocole devait posséder les qualités suivantes :

- une bonne reprise après panne
- la capacité à gérer un taux élevé d'erreurs
- une faible surcharge des données
- la capacité de se prolonger sans difficultés dans des sous-réseaux
- l'indépendance par rapport à un fournisseur particulier ou un type de réseau

A partir du 1er janvier 1983, seuls les paquets TCP/IP ont été transmis sur le réseau Arpanet (précurseur d'Internet). 1983 est donc en quelque sorte l'année de naissance d'Internet.

Il faut encore rajouter que TCP/IP se compose de deux protocoles distincts, IP et TCP.

Le protocole IP

Le Protocole Internet ou **IP (Internet Protocol)** est la partie la plus fondamentale d'Internet. Si vous voulez envoyer des données sur Internet, vous devez les "emballer" dans un *paquet IP*. La plupart du temps, ils ne peuvent pas contenir toute l'information qu'on voudrait envoyer sur Internet, et cette dernière doit par conséquent être fractionnée en de nombreux paquets IP.

Les paquets IP, outre l'information, sont constitués d'un en-tête contenant l'adresse IP de l'expéditeur (votre ordinateur) et celle du destinataire (l'ordinateur que vous voulez atteindre), ainsi qu'un nombre de contrôle déterminé par l'information emballée dans le paquet : ce nombre de contrôle, communément appelé *en-tête de total de contrôle*, permet au destinataire de savoir si le paquet IP a été "abîmé" pendant son transport.

L'adresse IP

Une des choses les plus intéressantes du protocole TCP/IP est d'avoir attribué un numéro fixe, comme un numéro de téléphone, à chaque ordinateur connecté sur Internet; ce numéro est appelé *l'adresse IP*. Dans le cadre du standard actuel - IPV4 -, les adresses sont codées sur 32 bits. Ainsi, tout ordinateur sur Internet se voit attribuer une adresse de type a.b.c.d (où a,b,c,d sont des nombres compris entre 0 et 255), par exemple 202.15.170.1. Dès ce moment, vous êtes le seul au monde à posséder ce numéro, et vous y êtes en principe directement atteignable.

Rappel : en théorie, un maximum de $256^4 = 4'294'967'296$ adresses possibles, ou, en d'autres termes, d'ordinateurs directement connectables, ce qui est plus que suffisant même à l'échelle mondiale (du moins à l'heure actuelle !).

En fait, il y a *beaucoup* moins d'adresses que ce nombre impressionnant, car de nombreux numéros IP ne sont pas autorisés ou sont utilisés à des fins "techniques".

4. Les différents types de réseaux

Une adresse IP est un nombre codé sur 4 octets. Par habitude, cette adresse est représentée sous la forme décimale pointée w.x.y.z où w,x,y,z sont quatre chiffres décimaux allant de 0 à 255. Cette adresse peut être vue de 2 façons différentes:

- La machine d'adresse w.x.y.z .

- La machine d'adresse z du réseau w.x.y.0 .
- La machine d'adresse y.z du réseau w.x.0.0 .
- La machine d'adresse x.y.z du réseau w.0.0.0 .

Ces différentes façons de lire une adresse IP permettent d'optimiser la façon de calculer les routes (routing, ou routage ???). La décomposition d'une adresse IP en adresse de réseau plus une adresse de machine sur un réseau ne se fait pas au hasard.

Les différentes classes d'adresses.

Pour voir si l'adresse du réseau d'une machine est codée sur 1,2 ou 3 octets, il suffit de regarder la valeur du premier. La valeur de l'octet x permet également de distinguer la classe du réseau.

Classe	Valeur de w	Lg Adresse Réseau	Nb de réseaux	nb max de machines
A	0 à 127	1 octet	127	16777216
B	128 à 191	2 octets	16384	65536
C	192 à 223	3 octets	2097152	255
D	224 à 239			
E	240 à 255			

La classe E est réservée pour des extensions futures.

La classe D est la classe de diffusion de groupe.

L'adressage a été structuré logiquement dans une architecture de réseaux et de sous-réseaux. N'importe qui ne peut s'approprier librement une adresse IP.

- Dans un réseau de classe A, l'Internic fixe les 8 bits de poids fort sous la forme 0xxxxxxx, les 24 autres bits sont laissés à l'administration de l'acquéreur du réseau de classe A. Dans un tel réseau, les adresses IP sont donc de type F.x.y.z où F (fixé par L'Internic) va de 0 à 126, les valeurs x,y et y étant laissées librement administrables par l'acquéreur. De grandes sociétés ont ce type de réseau; par exemple, Hewlett Packard possède le réseau 16.x.y.z (qu'on note aussi 16.0.0.0). Vous noterez que seuls 127 réseaux de ce type sont disponibles.
- Dans un réseau de classe B, l'Internic fixe les 16 premiers bits sous la forme 10xxxxxx yyyyyyyy, ce qui donne des réseaux de type F.G.0.0 où F (128-191) et G (0 à 255) sont fixés par le NIC.
- Dans un réseau de classe C, l'Internic fixe les 24 premiers bits sous la forme 110xxxxx yyyyyyy zzzzzzzz, ce qui donne des réseaux de type F.G.H.0 où F (192-223), G et H (0-255) sont fixés par le NIC.
- Tout le réseau 127.0.0.0 (qu'on peut voir comme un réseau de classe A) n'est pas attribué par l'Internic, car l'adresse 127.0.0.1, dite *adresse de boucle*, est réservée à des fins techniques. (24 millions d'adresses sont ainsi perdues !)
- De plus, l'Internic n'attribue pas non plus certains réseaux qui sont laissés à des fins privées. Ces plages d'adresses généralement non routées par les fournisseurs d'accès, en d'autres termes des plages attribuables tout à fait légalement pour des réseaux internes, vont

de	10.0.0.0	à	10.255.255.255
de	172.16.0.0	à	172.31.255.255
de	192.168.0.0	à	192.168.255.255

Typiquement, si vous créez votre propre réseau local en TCP/IP, vous utiliserez pour vos ordinateurs ce type d'adresses.

Il faut encore rajouter que certaines adresses d'un réseau quelconque ne sont pas attribuables à un ordinateur précis, mais joue un rôle "technique" dans TCP/IP.

Prenons l'exemple d'un réseau de classe C comme 192.168.0.x, x pouvant varier entre 0 et 255.

Cette plage d'adresses doit être indiquée de manière officielle, et on utilise pour cela l'adresse générale 192.168.0.0, ce qui veut dire "toutes les adresses comprises entre 192.168.0.0 et 192.168.0.255. Remarquez que cela signifie que vous ne pourrez jamais attribuer l'adresse 192.168.0.0 à un ordinateur précis, puisque cette dernière fait référence à tout le réseau.

Il existe une autre adresse IP réservée : *l'adresse de diffusion (broadcast)*. C'est la dernière adresse du sous réseau, dans notre cas 192.168.0.255. Il s'agit de l'adresse que vous utilisez pour diffuser un message vers chaque ordinateur du sous réseau concerné.

5. La subdivision en sous-réseaux

Comment un ordinateur transmet-il l'information (les paquets IP) à son destinataire ?

Une partie de la réponse se trouve dans le fonctionnement du protocole IP.

Généralement, un ordinateur ne peut transmettre directement un paquet IP qu'à un ordinateur situé sur le même sous réseau.

Par exemple, un ordinateur possédant l'adresse IP 192.168.0.2 pourra directement envoyer de l'information à un ordinateur "voisin" d'adresse 192.168.0.20, mais il ne pourra pas le faire avec un ordinateur d'adresse 194.38.175.55.

Pour simplifier, on dira en première approche qu'un ordinateur ne peut communiquer directement qu'avec un ordinateur possédant les trois premiers nombres de l'adresse IP identiques.

Cette remarque n'est malheureusement pas théoriquement juste (même si en pratique, c'est assez souvent le cas pour des réseaux simples). En fait, c'est le concept de *masque de sous-réseau* qui définit ce qu'un ordinateur peut "voir" ou ne pas voir.

Le masque de sous-réseau, si vous utilisez TCP/IP pour un réseau local, est 255.255.255.0. Ce masque veut dire que l'ordinateur concerné peut "voir" (ou communiquer avec) tous les ordinateurs possédant les trois premiers nombres de l'adresse IP identiques.

En fait, admettons que :

l'ordinateur A d'adresse IP 199.34.57.10 veuille envoyer un paquet IP à

l'ordinateur B d'adresse IP 199.34.57.20.

A priori, A ne sait pas s'il peut communiquer directement avec B. Pour cela, il utilise le masque de sous réseau 255.255.255.0 qu'on lui a imposé. Il "convertit" le tout en binaire, ce qui donne :

11111111	11111111	11111111	00000000	masque sous réseau
11000111	00100010	00111001	00001010	adresse de A
11000111	00100010	00111001	00010100	adresse de B

L'ordinateur A doit s'assurer que partout où le masque de sous réseau a une valeur de 1, la valeur binaire de son adresse IP corresponde à celle de B.

Dans l'exemple ci-dessus, il n'est pas difficile de voir que c'est le cas; finalement, les 8 derniers bits de valeur 0 indiquent que le dernier nombre de l'adresse IP est indifférent pour A, ce dernier verra donc tous les ordinateurs d'adresse 199.34.57.x, x étant compris entre 0 et 255.

De nombreux réseaux comportent des masques de sous réseaux moins compréhensibles (pas uniquement des 0 et des 255), comme par exemple 255.255.255.224. Si vous refaites le même raisonnement, vous verrez qu'avec un tel masque, l'ordinateur 192.168.0.2 ne peut directement communiquer avec l'ordinateur 192.168.0.100 ! En fait, les 256 adresses de ce réseau de classe C

seront comme subdivisées en 8 sous-réseaux de 32 ordinateurs.

Ainsi, les ordinateurs 192.168.0.0 à 192.168.0.31 pourront communiquer entre eux, de mêmes que les ordinateurs 192.168.0.32 à 192.168.0.63, les ordinateurs 192.168.0.64 à 192.168.0.95, les ordinateurs 192.168.0.96 à 192.168.0.127, les ordinateurs 192.168.0.128 à 192.168.0.159, les ordinateurs 192.168.0.160 à 192.168.0.191, les ordinateurs 192.168.0.192 à 192.168.0.223, les ordinateurs 192.168.0.224 à 192.168.0.255, mais ces sous-réseaux ne pourront pas communiquer directement entre eux.

Cette subdivision d'un réseau de classe C en plusieurs sous-réseaux peut être utile pour un fournisseur d'accès. Vous pouvez calculer aisément les masques de sous-réseaux suivants selon le nombre de sous réseaux que vous souhaitez créer.

nombre de sous réseaux	IP par sous réseau	masque de sous réseau
1	256	255.255.255.000
2	128	255.255.255.128
4	64	255.255.255.192
8	32	255.255.255.224
16	16	255.255.255.240
32	8	255.255.255.248

En fait, nous avons vu au paragraphe précédent que pour chaque sous réseau il faut déduire trois adresses IP non attribuables à un ordinateur :

1. l'adresse de sous réseau (généralement le premier IP du sous réseau), par exemple a.b.c.0 pour un réseau composé d'un seul sous-réseau, ou a.b.c.64 pour le troisième sous-réseau d'un réseau divisé en 8 sous-réseaux.
2. l'adresse de diffusion (généralement le dernier IP du sous-réseau), par exemple, en reprenant les deux exemples précédents, a.b.c.255 ou a.b.c.95.

Chaque sous-réseau "perd" donc trois adresses IP. Il s'ensuit qu'une subdivision excessive d'un réseau n'est pas avantageuse (on divise rarement au-delà de 8 sous-réseaux).

6. Le routage des paquets IP et le protocole TCP

Revenons à notre ordinateur A d'adresse 192.168.0.2 (mettons-lui un masque de sous-réseau de 255.255.255.0). Admettons qu'il veuille envoyer un paquet IP à ordinateur B d'adresse 192.170.0.4. En utilisant le masque de sous-réseau, A comprend qu'il ne peut atteindre directement B. Que fait-il donc ?

Il envoie sans réfléchir le paquet IP à l'adresse du routeur par défaut (disons que ce dernier a été défini comme 192.168.0.254).

Qu'est-ce que ce *routeur* ? Le routeur est une machine pouvant "jouer sur plusieurs sous-réseaux" en même temps. Typiquement, si on utilise un ordinateur, ce dernier possèdera deux cartes réseaux (ou plus), l'une connectée sur l'un des sous-réseaux (dans notre cas, disons qu'elle possède l'adresse 192.168.0.254), l'autre connectée sur l'autre sous-réseau (disons 192.170.0.192). S'il utilise le bon logiciel, un tel ordinateur est capable de faire transiter des paquets IP du réseau 192.168.0.0 vers le réseau 192.170.0.0, et inversement bien sûr.

Deux petites remarques s'imposent. Tout d'abord, c'est donc grâce à des routeurs que différents sous-réseaux d'un réseau de classe C peuvent communiquer entre eux, par exemple l'ordinateur 192.168.0.2 avec l'ordinateur 192.168.0.120 d'un réseau de classe C subdivisé en 8 sous-réseaux (masque de sous réseau 255.255.255.224). La seconde remarque est d'ordre plus pratique : vous retiendrez que Windows 95 n'est pas capable de faire du routage, bien qu'il soit tout à fait possible

d'installer deux cartes réseaux (avec des IP différents) dans un ordinateur tournant sous ce système; par contre, Windows NT 4.0, même en version Workstation, est capable d'une telle fonction.

Question pertinente : pourquoi subdiviser et ne pas faire de "méga" réseaux ? Les deux points suivants expliquent en partie pourquoi on procède ainsi.

1. Limiter le trafic sur un tronçon donné. Imaginons deux réseaux locaux A et B séparés par un routeur. Lorsque des ordinateurs de A discutent avec des ordinateurs de B, le routeur a pour rôle de transmettre l'information du réseau A vers le réseau B (et inversement). Par contre, si des ordinateurs de A s'échangent entre eux des données, il n'y a pas de raison qu'ils encombrant inutilement le trafic sur le réseau B, et c'est bien pour cette raison que les réseaux A et B sont distincts.
Autre évidence : si le réseau A tombe en panne, le réseau B n'en est pas affecté. C'est d'ailleurs l'avantage principal de subdiviser : éviter qu'un ennui technique qui pourrait rester localisé ne perturbe la totalité du réseau
2. Autre aspect non négligeable : le *broadcast (diffusion)*. Dans notre dos, les ordinateurs sont de grands bavards : ils ne cessent de causer entre eux pour signaler leur présence ou se mettre d'accord sur les protocoles qu'ils sont capables de comprendre. Pensez un peu si Internet n'était constitué que d'un seul segment. Le broadcast seul des ordinateurs utiliserait l'intégralité de la bande passante avant même qu'un seul octet de données ait pu être transmis ! Pour cette raison, le travail des routeurs est non seulement de faire transiter les paquets IP, mais aussi de **filtrer** le broadcast local qui n'intéresse pas la planète entière. Vous comprendrez par là que les routeurs jouent un rôle essentiel pour éviter la saturation du trafic.

Lorsqu'un ordinateur doit acheminer un paquet IP, il vérifie tout d'abord s'il peut le transmettre directement (grâce au masque de sous-réseau), s'il ne peut pas, il l'envoie bêtement, sans réfléchir, au routeur par défaut. A partir de là, les routeurs sont généralement configurés pour savoir où diriger les paquets IP qui leur sont confiés, les routeurs bavardent entre eux (à l'aide de protocoles particuliers de routage, RIP ou OSPF par exemple) pour savoir quelle est la meilleure route (la plus courte généralement) pour qu'un paquet IP atteigne sa destination. De même, si une route est soudainement interrompue, les routeurs sont capables de se reconfigurer et proposer des nouvelles routes de secours.

Or le protocole IP néglige un point crucial : il ne vérifie nullement le bon acheminement des paquets IP. En d'autres termes, l'ordinateur expéditeur, dans le protocole IP, ne fait qu'envoyer le paquet IP plus loin; il ne s'intéresse pas du tout de savoir si le paquet a bien été reçu ou s'il a été endommagé pendant le transfert !

Qui doit donc assurer l'intégrité point à point, si ce n'est IP ? La réponse : son copain, TCP.

On résume rapidement les principales fonctionnalités du protocole TCP ainsi :

- l'établissement d'une liaison
- le séquençage des paquets
- le contrôle de flux
- la gestion d'erreurs
- le message d'établissement d'une liaison

On entend par "contrôle de flux" la capacité de TCP, entre autres, de reconstituer l'information originale à partir de paquets IP arrivés (souvent) dans le désordre le plus absolu.

7. Le système de désignation de noms (DNS) Domain Name System

Nous avons vu plus haut que tout ordinateur connecté à Internet possède un numéro IP qui lui est propre. Pour communiquer avec un autre ordinateur, il vous faut connaître son adresse IP. Or,

lorsque vous "surfez" sur le net, vous écrivez très rarement de tels numéros dans votre browser. C'est tout simplement que vous faites appel, sans le savoir, à un serveur DNS.

Un serveur DNS est simplement une machine qui associe le numéro IP à une adresse plus facilement mémorisable, bref une sorte d'annuaire téléphonique pour Internet.

Ainsi, la machine qui répond lorsque vous tapez `http://www.microsoft.com` dans votre browser possède en fait l'adresse IP 207.68.137.65. Si vous tapez `http://207.68.137.65`, vous obtiendriez exactement le même résultat. Un (ou plusieurs) serveur DNS se trouvent généralement chez votre provider.

Une manière simple de constater l'utilité d'un serveur DNS est d'ouvrir (sous Windows 98 ou XP) une fenêtre DOS, et de taper `ping 'adresse de l'hôte'`, par exemple `ping www.google.fr`. "Ping" est une fonction très utile dans l'établissement de réseau : c'est une commande qui envoie un paquet IP tout simple à un ordinateur et lui demande simplement de répondre. Sous Windows 98, quatre paquets IP sont envoyés, et si vous avez tapé `'ping www.google.fr'` par exemple, votre ordinateur devrait ensuite vous écrire une ligne de type :
`pinging www.google.fr [66.102.9.99] with 32 bytes of data`
suivie de quatre lignes de la forme :
`reply from 66.102.9.99: bytes=32 time=550ms TTL=128`

Ces quatre dernières lignes vous indiquent que le serveur google a répondu à vos appels et vous montrent le temps total qu'a pris la transaction pour chaque ping (par exemple 550 millisecondes). Vous noterez surtout que le serveur DNS de votre provider aura fait automatiquement la translation `www.google.fr` <-> `66.102.9.99`.

PS : Nous avons parlé plus haut de l'adresse IP réservée 127.0.0.1, dite adresse de boucle, un ping sur cette adresse correspond à un ping "sur soi-même", ce qui permet de tester la bonne marche de la carte réseau.

8. Résumé et exemples

Résumons en quelques points ce que nous avons vu sur les réseaux TCP/IP.

1. Chaque ordinateur sur Internet possède une adresse IP, par exemple 195.235.4.6
2. Les adresses IP définissent les termes de réseaux ou de sous réseaux. C'est un organisme international, l'Internic, qui attribue les différentes adresses ou les différents réseaux (classe A, B, C). Ce sont ensuite les entreprises qui ont acheté les réseaux qui peuvent les subdiviser en sous réseaux grâce à l'utilisation de masques de sous réseaux adéquats.
3. De nombreuses adresses IP ne sont pas utilisées.
 - L'Internic tout d'abord conserve des adresses utilisables à des fins privées, par exemple les adresses de type 192.168.0.x
 - L'administrateur d'un réseau doit toujours mettre de côté trois adresses IP par sous réseau : l'adresse de sous réseau (par exemple 192.168.0.0), l'adresse de diffusion (par exemple 192.168.0.255) et l'adresse du routeur par défaut.
4. Pour communiquer, l'ordinateur expéditeur fragmente l'information à envoyer en de nombreux paquets IP qui contiennent, outre l'information, les adresses IP de l'expéditeur et du destinataire ainsi qu'un en-tête de total de contrôle.
5. Les paquets IP ne peuvent être transmis directement qu'à un ordinateur du même sous réseau (défini par le masque de sous réseau). Si l'ordinateur destinataire ne peut être atteint, l'ordinateur expéditeur envoie le paquet IP à l'adresse du routeur par défaut qui lui a été spécifié.
6. Le routeur est une machine qui fait transiter les paquets d'un réseau à un autre (ou d'un sous réseau à un autre) et qui utilise donc plusieurs adresses IP (une sur chacun des sous réseaux couverts). Par exemple, un routeur possédant les deux adresses IP 196.129.0.1 et

197.160.40.91 peut faire passer des paquets IP du réseau 196.129.0.0 au réseau 197.160.40.0, et inversement.

7. Le protocole IP ne s'occupe que de l'acheminement des paquets IP. La vérification du transfert de l'intégrité des données est effectuée par le protocole TCP.