

## GENERALITES

TCP/IP est un protocole inventé par les créateurs d'Unix. (Transfer Control Protocol / Internet Protocole).

TCP/IP est basé sur le repérage de chaque ordinateur par une adresse appelée *adresse IP* qui permet d'acheminer les données à la bonne adresse. Avec ce protocole on trouve d'autres protocoles permettant de faire les choses suivantes :

- [IRC](#): discuter en direct
- [http](#): regarder des pages web
- [ftp](#): transférer des fichiers
- et bien d'autres choses

Comme on peut faire différentes choses en même temps, il faut déterminer à quel programme on a faire. Pour cela, on assigne à chacun d'entre eux un numéro ([le port](#)) qui est transmis lors de la communication (la transmission est effectuée par petits paquets d'informations). Ainsi on sait à quel programme correspond chaque petit paquet. Par exemple les paquets http arrivent sur le port 80, les paquets irc arrivent sur le port 6667 (ou un autre situé généralement autour de 7000) et ftp sur le port 21.

## L'ADRESSE IP

L'adresse IP est codé sur 32 bits, soit sur 4 numéros allant de 0 à 255 (4 fois 8 bits), on les note donc sous la forme xxx.xxx.xxx.xxx où chaque xxx représente un entier de 0 à 255.

Ces numéros servent aux ordinateurs du réseau pour se reconnaître, ainsi il ne doit pas exister deux ordinateurs sur le réseau ayant la même adresse IP.

194.153.205.26

On distingue en fait deux parties dans l'adresse IP :

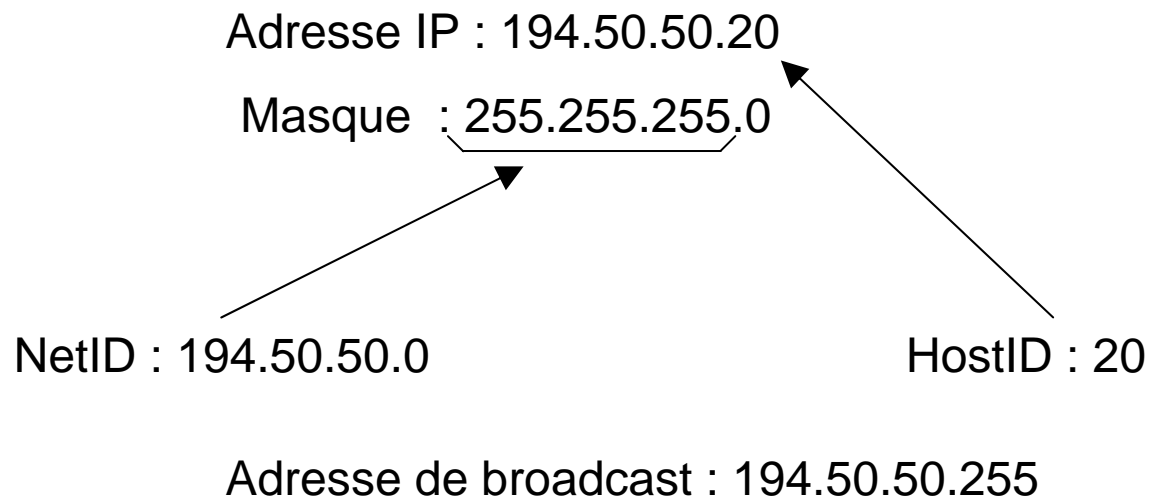
- une partie des nombres à gauche désigne le réseau (on l'appelle *netID*)
- les nombres à droite restant désignent les ordinateurs de ce réseau (on l'appelle *host-ID*)

Pour connaître quelle partie il faut connaître aussi le masque de sous réseaux. Celui-ci composé aussi de 4 numéros allant de 0 à 255 correspond à 4 fois 8 bits. Les 1 indique l'id réseaux et il faut faire une opération binaire avec l'adresse IP pour connaître le nombre de netID possible. Voici un programme spécialisé [ShuntIPCalculator](#)

## ADRESSE IP

Par exemple le masque 255.255.255.0 pour une adresse IP 194.50.50.20 nous donne un NetID de 194.50.50 et un HOSTID de 20.

Dans ce cas on aura 254 machines possible car de 0 à 255 se fait 256 possibilités mais il faut savoir que 194.50.50.0 est l'adresse du réseau (NetID) et 194.50.50.255 est l'adresse de diffusion (broadcast) qui permet d'envoyer un message à l'ensemble de toutes les machines du réseau dont on obtient au final 254 machines maxi.



## CLASSE

Cette notion de 254 machines s'appelle une classe. Voici des exemples de classes :

Classe	Nombre de réseaux possibles	Nombre d'ordinateurs maxi sur chacun
A	126	16777214
B	16384	65534
C	2097152	254

Il y a aussi des classes d'adresse réservées pour des usages privés et notamment pour des réseaux internes aux entreprises.

10.0.0.1 à 10.255.255.254  
172.16.0.1 à 172.31.255.254  
192.168.0.1 à 192.168.255.254

## DNS

Les adresses IP sont des numéros et il est difficile de les retenir s'est pourquoi on peut faire une correspondance entre une adresse ip et un nom. On parle de nom de machine (Host Name).

Au début il y avait très peu de machines et on faisait un fichier qui rassemblait tous les noms. Il est composé de l'adresse IP suivi de son nom. Ce fichier s'appelle hosts et il doit se trouver sur chaque machine.

Maintenant avec beaucoup de machines on fait une base de données centralisée qui fait la même chose mais de manière automatique. Cela s'appelle un serveur de nom de domaine (Domain Name Server).

Si on a a faire à des sites Web il y a en plus un suffixe du style .fr .com .net ,etc



## DHCP et PORT

### DHCP

Si nous avons beaucoup de machines il faut aussi se creuser la cervelle pour trouver des adresses IP. On peut le faire automatiquement via un serveur qui délivre automatiquement des adresses.

Dynamic Host Control Protocol

### PORT

Il y a au total 65536 ports et s'est l'IANA (*Internet Assigned Numbers Agency*) qui est chargée de les gérer. Voici une liste simplifié :

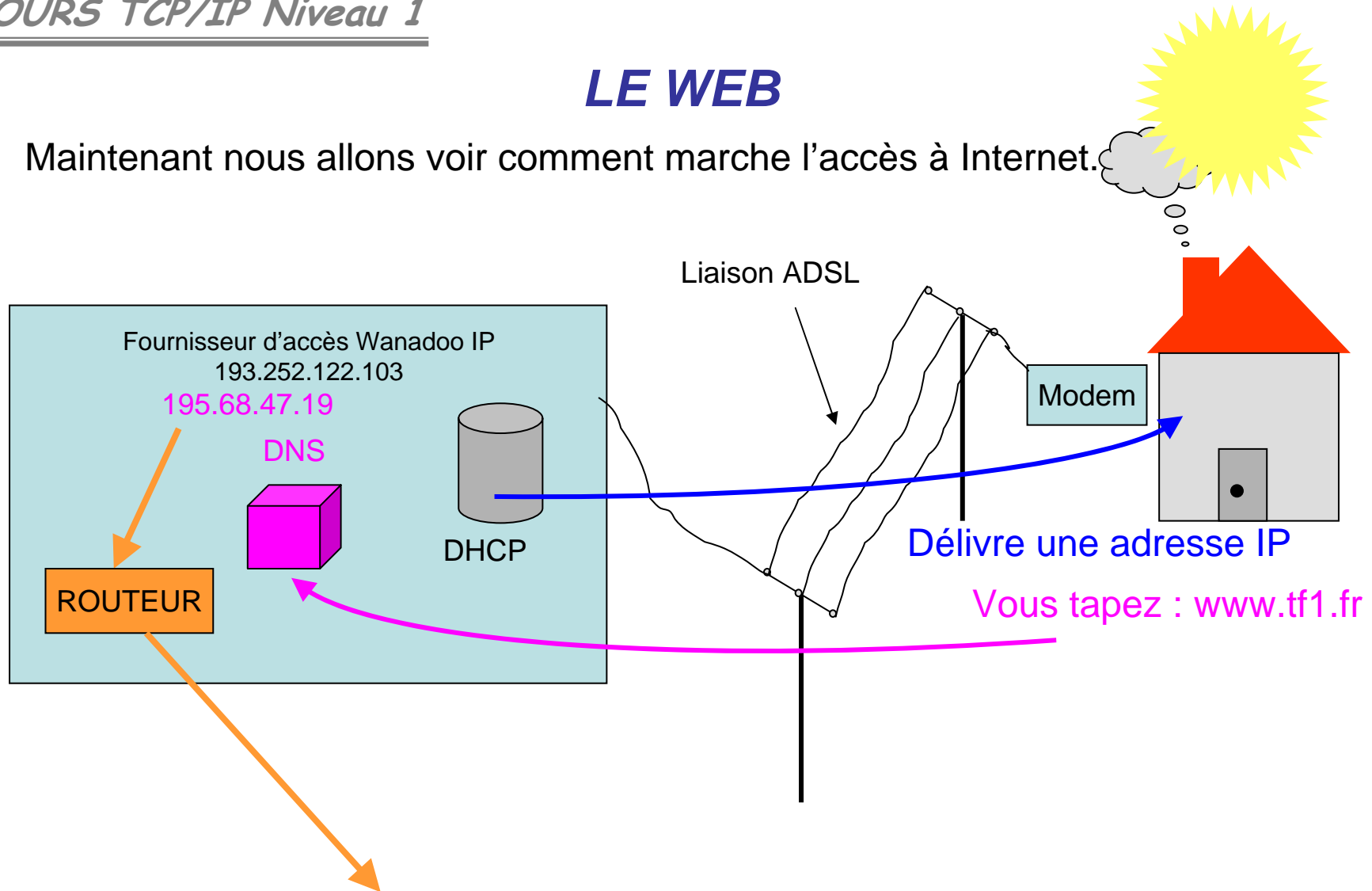
Port	Application
21	FTP
23	TELNET
25	SMTP
53	DNS
63	WHOIS
70	GOPHER
79	FINGER
80	HTTP
110	POP3
119	NNTP

Site internet pour liste complète :

<http://www.iana.org/assignments/port-numbers>

## LE WEB

Maintenant nous allons voir comment marche l'accès à Internet.



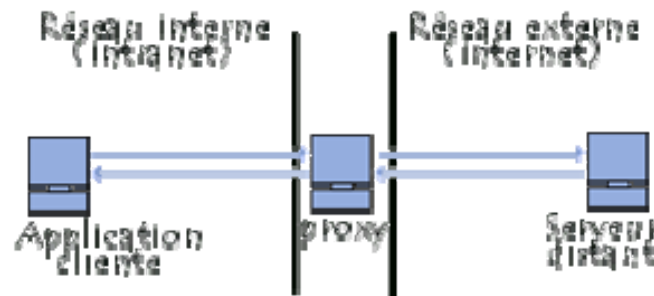
On arrive sur le serveur qui accueille les pages Web de tf1.fr (en Hollande) et retour à la maison via le port 80

## LE WEB

### PROXY

Un **proxy** (traduction française de «*proxy server*», appelé aussi «*serveur mandataire*») est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau et Internet.

Le fonctionnement d'un proxy est assez simple : Lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.



## LE WEB

### La fonction cache

Les proxys assurent la fonction de **cache** (en anglais *caching*), c'est-à-dire la capacité à garder en mémoire (en "cache") les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible. Toutefois, pour mener à bien cette mission, il est nécessaire que le proxy compare régulièrement les données qu'il stocke en mémoire cache avec les données distantes afin de s'assurer que les données en cache sont toujours valides.

### Le filtrage

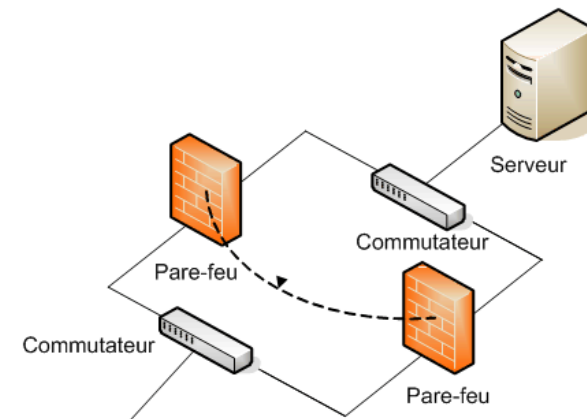
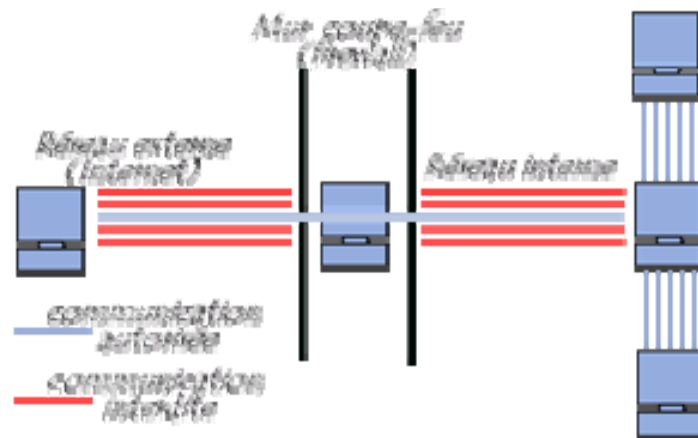
Il est possible d'assurer un suivi des connexions (en anglais *logging* ou *tracking*) via la constitution de journaux d'activité (*logs*) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.

Il est ainsi possible de filtrer les connexions à Internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs.

## LE WEB

### Firewall

Un **pare-feu**, est un système permettant de protéger un ordinateur des intrusions provenant du réseau (ou bien protégeant un réseau local des attaques provenant d'Internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante.



## **LE WEB**

Un firewall fonctionne sur le principe d'autoriser uniquement les communications ayant été explicitement autorisées.

Il effectue un filtrage de paquets et analyse les en-têtes de chaque paquet échangé entre une machine du réseau local et une machine extérieure sachant que chaque paquet contient :

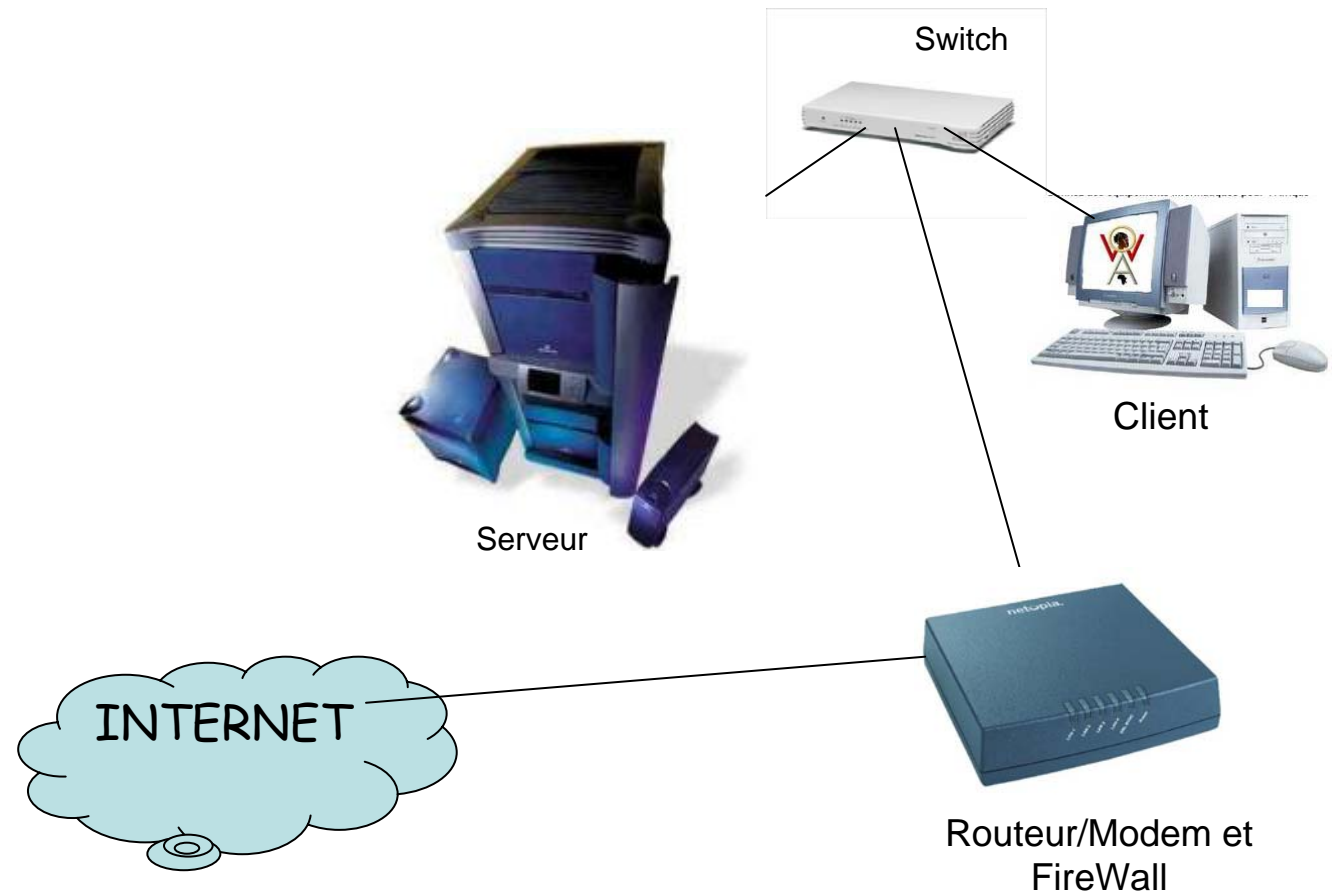
- adresse IP de la machine émettrice
- adresse IP de la machine réceptrice
- type de paquet
- numéro de port

Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables (selon la politique de sécurité retenue).

Le port 23 est par exemple souvent bloqué par défaut par les dispositifs pare-feu car il correspond au protocole Telnet.

## LE WEB

Schéma typique d'un petit réseau connecté à Internet.



## LE WEB

Schéma typique d'un gros réseau connecté à Internet.

