Les réseaux informatiques

Université Nice SOPHIA ANTIPOLIS

Les réseaux informatiques: définition

Le terme générique « réseau » définit un ensemble d'entités (objets, personnes, etc.) interconnectées les unes avec les autres. Un réseau permet ainsi de faire circuler des éléments matériels ou immatériels entre chacune de ces entités selon des règles bien définies.

-> réseau informatique: ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques.

Les réseaux informatiques: définition

Un ordinateur est une machine permettant de manipuler des données. L'homme, en tant qu'être communiquant, a rapidement compris l'intérêt qu'il pouvait y avoir à relier ces ordinateurs entre-eux afin de pouvoir échanger des informations.

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)
- Le jeu vidéo multijoueurs
- Objets “connectés”

Similitudes entre types de réseaux

Les différents types de réseaux ont généralement les points suivants en commun :

- Serveurs : ordinateurs qui fournissent des ressources partagées aux utilisateurs par un serveur de réseau

- Clients : ordinateurs qui accèdent aux ressources partagées fournies par un serveur de réseau

- Support de connexion : conditionne la façon dont les systèmes sont reliés entre eux.

- Données partagées : Fichiers, imprimantes ou autres périphériques utilisés et partagés par les usagers du réseau

- Ressources diverses : autres ressources fournies par le serveur (processus de calculs communs, etc.)

Les différents types de réseaux

On distingue différents types de réseaux selon leur taille (en terme de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue.

On fait généralement trois catégories de réseaux :

- LAN (local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

Les différents types de réseaux

Les LAN

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps et 1 Gbps environ.

La taille d'un réseau local varie de 2 à quelques centaines de machines (généralement une dizaine maximum).

Typiquement une ou plusieurs salles (exemple de la salle de TD) ou bureaux

En élargissant le contexte de la définition aux services qu'apportent le réseau local, il est possible de distinguer deux modes de fonctionnement :

- dans un environnement d'"égal à égal" (en anglais peer to peer), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur a un rôle similaire
- dans un environnement "client/serveur", dans lequel un ordinateur central fournit des services réseaux aux utilisateurs

Les différents types de réseaux

Les MAN

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) mais généralement <1 km^2, à des débits importants. Ainsi un MAN permet à deux noeuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

Par exemple, un lycée ou une université

Les technologies pour assurer de bon débits sont principalement le Gigabit Ethernet et le 10 Gigabit Ethernet.

Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

Les différents types de réseaux

Les WAN

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs et/ou WAN à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un noeud du réseau.

Le plus connu des WAN est Internet.

Le Réseau Internet

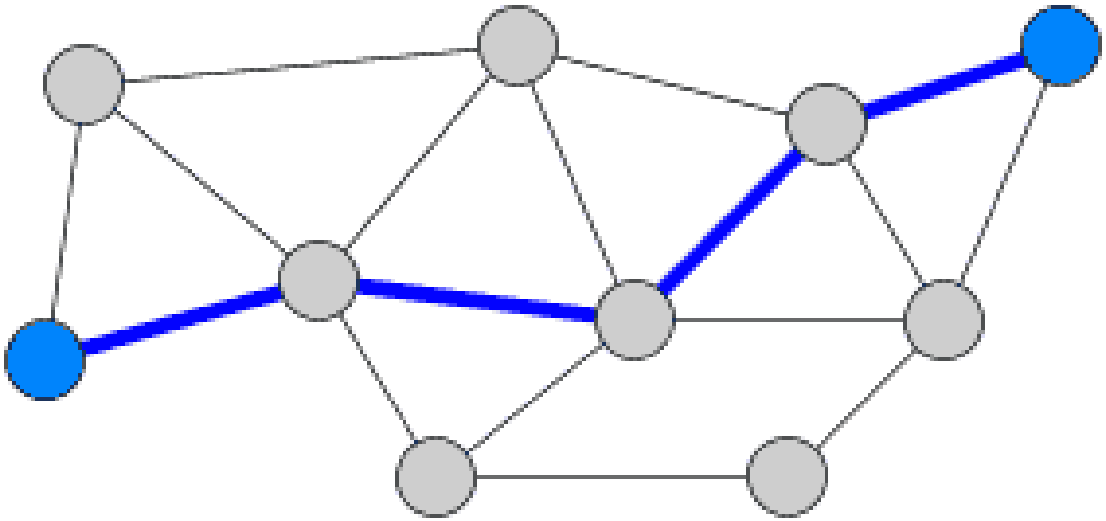
Internet est la suite du réseau militaire américain ARPANET.

Le but était de concevoir un réseau résistant aux attaques : les communications ne passent plus selon un mode linéaire, mais peuvent à chaque endroit emprunter plusieurs routes.

Les informations peuvent continuer à circuler, même en cas de destruction majeure d'une partie du territoire (on est en pleine guerre froide).

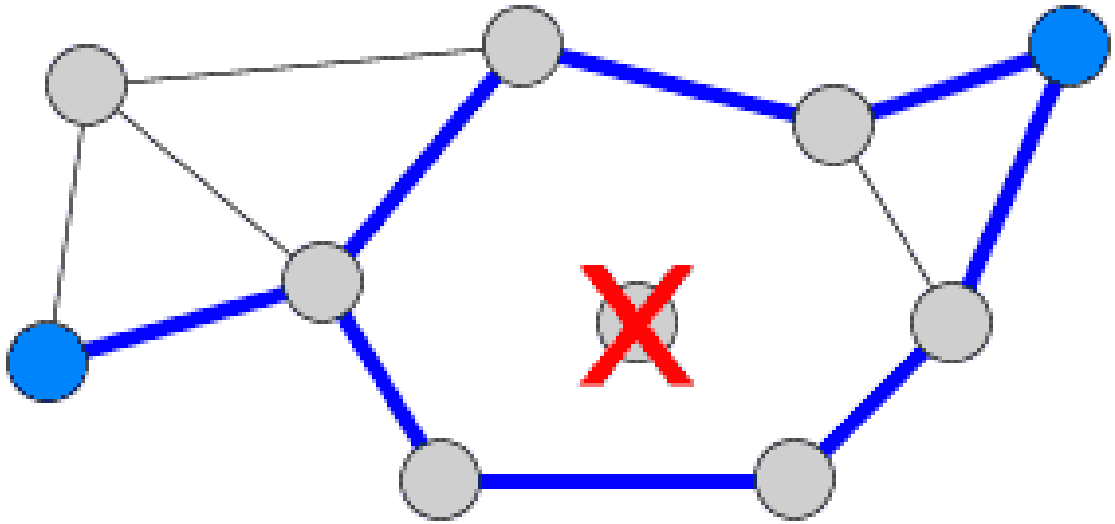
Internet a donc été conçu dès l'origine comme une toile d'araignée, d'où son nom anglais web (qui veut dire tissage et toile d'araignée).

Fonctionnement



Cas normal, tout fonctionne correctement, les informations empruntent le "chemin le plus direct".

Fonctionnement



En cas de disfonctionnement : un relais ne fonctionne plus, il existe alors au moins une autre possibilité pour acheminer les informations.

Le Réseau Internet

L'interconnexion progressive de tous les ordinateurs de la planète fonctionne donc comme un gigantesque réseau. Le mot anglais pour réseau est "network".

Or dans la pratique, ces ordinateurs ne sont pas directement interconnectés entre eux. Les ordinateurs sont d'abord interconnectés au sein d'un institut ou d'un batiment formant ainsi une multitude de petits sous-réseaux. Puis par sous réseau une machine est chargée de s'interconnecter avec d'autres machines.

Enfin progressivement la planète entière est interconnectée avec à chaque étape du maillage une machine désignée pour se connecter au niveau supérieur. On a ainsi une interconnexion de toutes les machines par interconnexion de réseaux successifs.
D'où le terme Internet pour "INTER-NETworks".

Gestion des connexions

Chaque ordinateur connecté directement sur Internet possède un numéro d'identification unique (appelée adresse IP) et peut envoyer et recevoir des informations avec n'importe quel autre ordinateur ou machine possédant une adresse IP (voire même une imprimante).

Par ailleurs, le temps d'acheminement ne dépend pas de la distance, mais plutôt de la qualité des lignes qui séparent deux machines.

Notons que vous pouvez être reliés à Internet sans disposer de votre propre adresse IP. Il faut faire appel à un serveur (FAI) qui vous en attribue une pour votre connexion.

Gestion des connexions

Ce réseau mondial utilise les mêmes protocoles de communication (exemple TCP/IP) et fonctionne comme un réseau virtuel unique et coopératif.

Tous les ordinateurs et logiciels supportant les mêmes protocoles pourront communiquer ensemble.

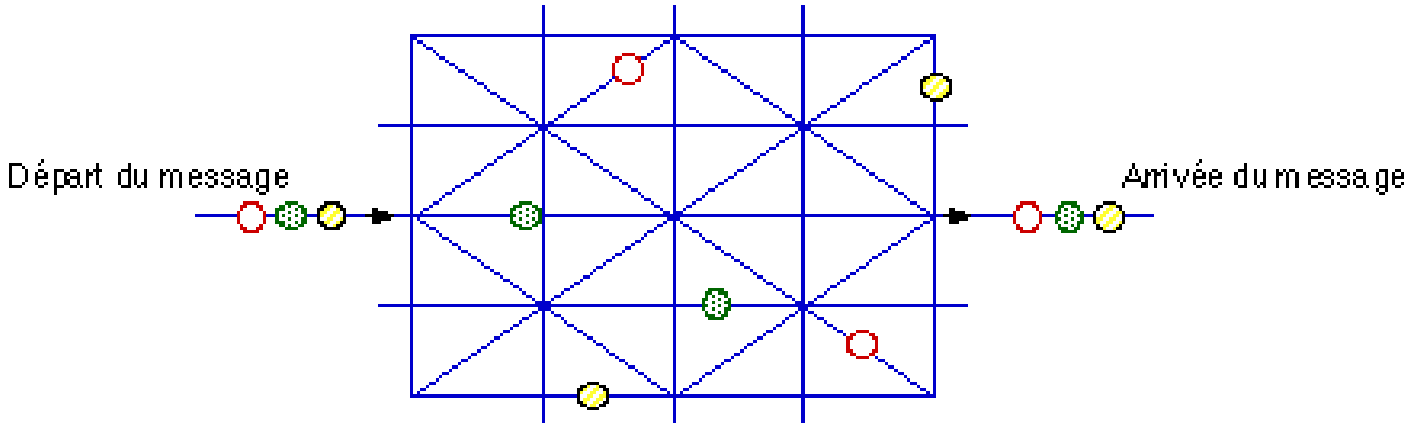
Internet utilise un système international d'adresses qui permet d'envoyer un message ou un fichier sans ambiguïté à un correspondant connecté.

Chaque ordinateur a une adresse unique.

-> Principe du réseau décentralisé et redondant.

Le Réseau Internet

Le transfert de données



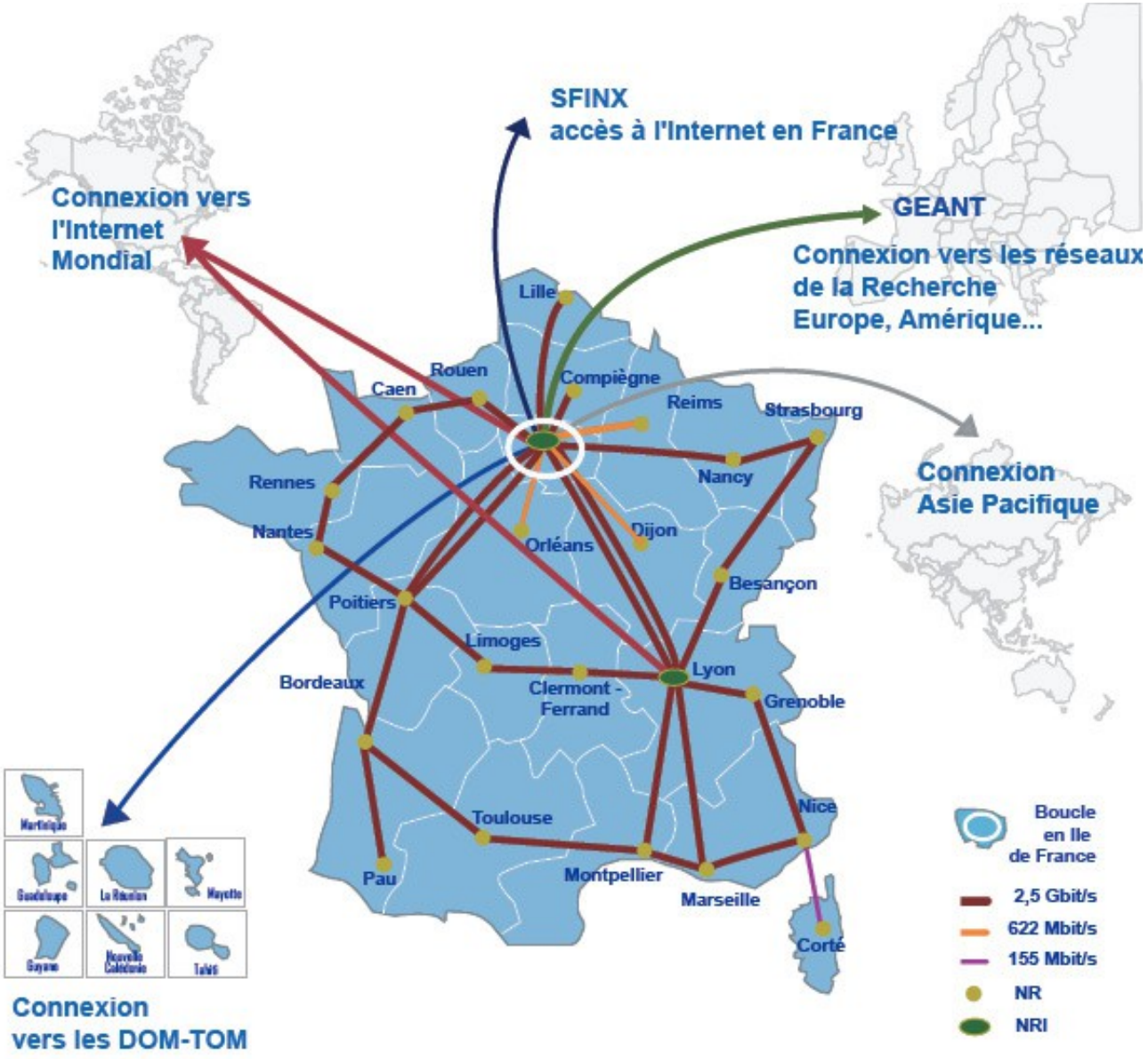
Chaque ordinateur constitue un nœud du réseau. Il est identifié par une adresse IP (Internet Protocole) qui est son identificateur.

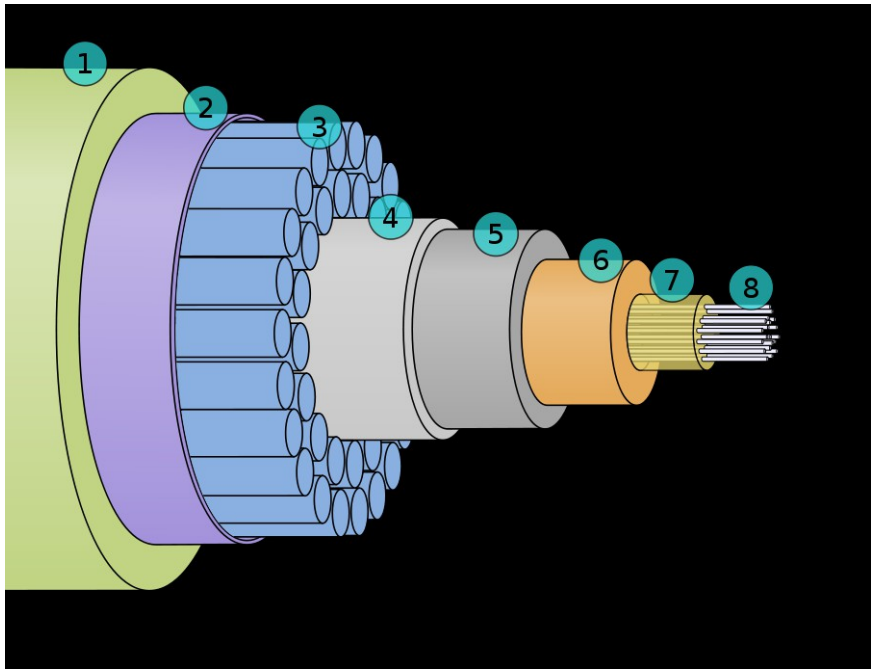
Chaque noeud a un certain nombre de voisins. Une table en chaque nœud indique les voisins possibles.

L'information est coupée en paquets. Ces paquets sont routés indépendamment sur le réseau et reconstitués à l'arrivée.

Le calcul du parcours se fait de façon dynamique (dépend de l'encombrement du réseau). Les messages circulent sur le réseau, sur chacun est indiqué le nom du destinataire, le nom de l'expéditeur.

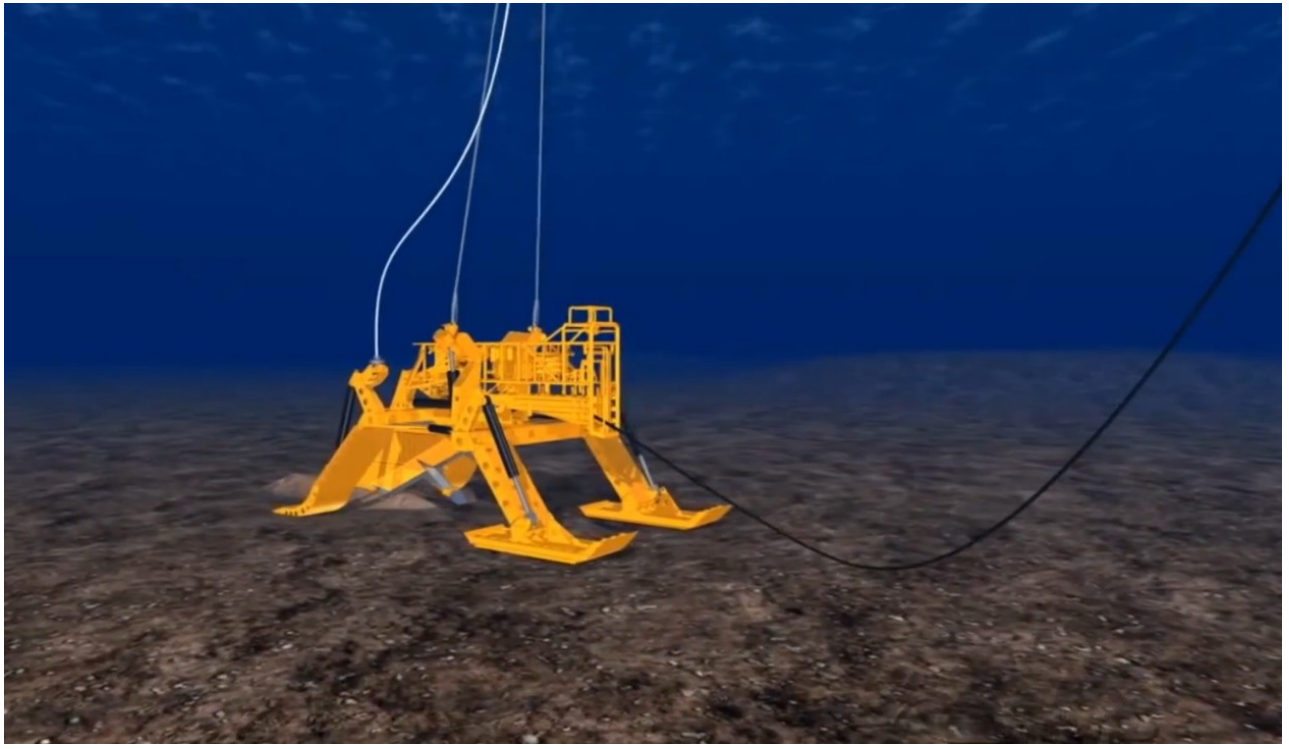
RENATER (réseau national de télécommunications pour la technologie, l'enseignement et la recherche) est le réseau informatique français reliant les différentes universités et les différents centres de recherche entres eux en France





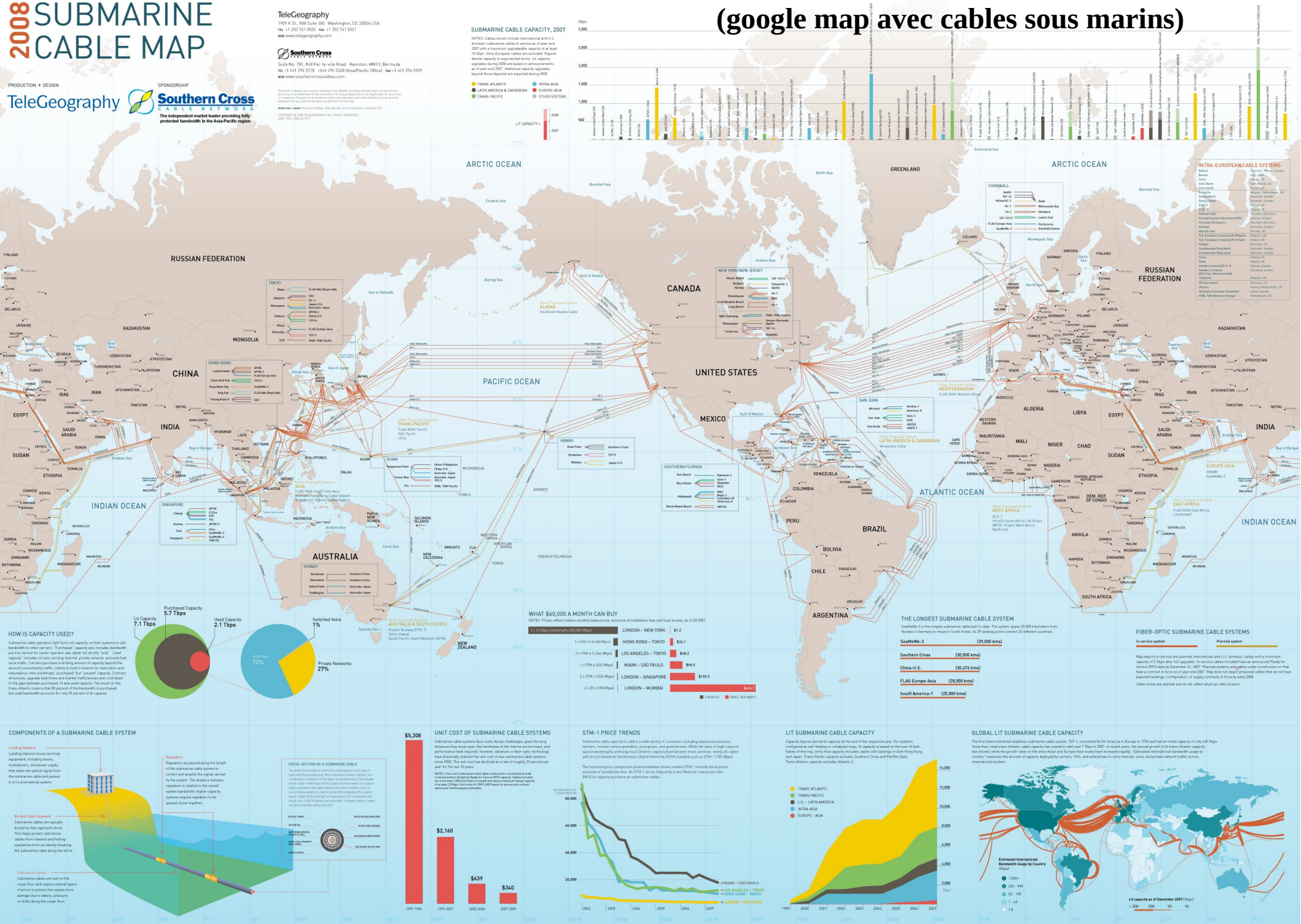
A cross section of a modern submarine communications cable.

1 – Polyethylene
2 – Mylar tape
3 – Stranded steel wires
4 – Aluminium water barrier
5 – Polycarbonate
6 – Copper or aluminium tube
7 – Petroleum jelly
8 – Optical fibers



Source : https://www.telegeography.com

A voir : http://www.submarinecablemap.com (google map avec cables sous marins)



Internet ne se limite pas aux pages web !

Les utilisations d'Internet que vous connaissez bien sont les pages web que vous voyez dans votre navigateur et l'envoi et la réception d'e-mails.

L'utilisation des pages web repose sur ce qu'on appelle le protocole http (utilisé par votre navigateur) qui permet le transport des pages html, des images (jpeg, gif...), musiques (MP3...), vidéos...

Mais Internet ne se limite pas aux pages web !

Il existe beaucoup d'autres protocoles qui servent à d'autres utilisations.

Les protocoles

Un protocole est une méthode standard qui permet la communication entre deux machines :

=> Ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur le réseau.

Ethernet => depuis cable réseau

IP => le protocole "IP"(Internet Protocol) nécessite une adresse "IP"

UDP, TCP => User Datagram Protocol /Transmission Control Protocol

HTTP, FTP, SMTP, … => les derniers protcoles qui sont envoyés aux navigateurs, clients mails, etc.

Adresse IP : utilise des numéros de 32 bits (4 fois 8 bits, 4 octets donc) que l'on écrit sous forme décimale donc 4 nombres allant de 0 à 255 : "xxx.xxx.xxx.xxx" exemple : "134.59.1.69"

Sur 4 octets, en tout environ 4 milliards d'adresses différentes

Internet aujourd'hui

Jamais les inventeurs d'Internet n'ont imaginé toutes les applications qui existent aujourd'hui sur Internet.

Il est maintenant question de relier tous vos appareils entre eux par Internet : téléphone, matériel hi-fi, réfrigérateur, chauffage, les voitures… le tout « numérique » ou tout « connecté »)

Mais cela veut dire qu'il faut suffisamment d'adresses IP pour en donner une à chaque machine. Tout comme pour le téléphone, personne n'avait prévu au départ le nombre astronomique d'adresses IP dont il faudrait disposer dans le futur.

Application MyBosch.

Internet aujourd'hui

La version 4 ("IPv4") du protocole IP est toujours la plus utilisée pour permettre aux machines de dialoguer entre elles. Mais il existe des problèmes :

- Manque d'adresses IP.
- Vitesses de transmission trop faibles devant des fichiers de plus en plus gros (videos).
- Manque de sécurité (spams, virus...).

Pour résoudre ces problèmes IPv6 prend le relais.

Le problème majeur est que IPv6 n'est pas directement compatible avec IPv4. Il est prévu un basculement graduel vers IPv6.

Les systèmes d'exploitation modernes (Unix, Linux, MacOS, Windows, Android, ...) sont tous capables de comprendre IPv6.

Au début de l'année 2016, le déploiement d'IPv6 est encore limité, la proportion d'utilisateurs Internet en IPv6 étant estimée à 10 %4, et ce en dépit d'appels pressants à accélérer la migration adressés aux fournisseurs d'accès à Internet et aux fournisseurs de contenu ...l'épuisement des adresses IPv4 publiques disponibles étant imminent. ***https://fr.wikipedia.org/wiki/IPv6***

• **FTP** sert à transférer des fichiers d'un ordinateur à l'autre de manère optimale (**SFTP** equivalent crypté).

• **IRC/ ICQ** permet de créer des «salons» de discussion ou des "tchats"

• **NTP** permet de mettre les ordinateurs à l'heure par internet à 500 millisecondes près.

• **P2P** permettent de partager des fichiers à grande échelle (en fait il existe plusieurs protocoles P2P).

• **NNTP** permet d'accéder à des forums de discussion sur des milliers de sujets différents (=Usenet, newsgroup).

• **TELNET** permet de commander un ordinateur distant, c'est à dire de lancer des commandes, depuis son ordinateur. **SSH** idem TELNET, mais permet d'avoir un accès à des ordinateurs distants de manière cryptée.

• **SMTP** (Simple Mail Transfer Protocol) permet d'envoyer des emails

• **POP3** permet de recevoir les mails (existe aussi le protocle **IMAP** comme équivalent).

• **HTTP** protocole pour recevoir les pages web dans un navigateur (équivalent crypté : **HTTPS**)

• **ICMP** (Internet Control Message Protocol) permet de controler la connectivité des machines sur un réseau et de détecter d'eventuelles erreurs, soit parceque non connectées au net, soit des problèmes de lenteur de la connexion. Commande la plus connu du protocole : "ping"

Quelques commandes réseaux

Ping adresse_IP ex. : ping 134.59.204.1

Ping utilise le protocole ICMP (Internet Control Message Protocol).

Vérifie la connectivité IP d'un ordinateur en envoyant des messages (requête écho) dans le but d'avoir des réponses d'une machine.
Les réponses à la requête écho, s'affichent, avec les temps de l'aller-retour (ping-pong)

Ping est la principale commande TCP/IP utilisée pour résoudre les problèmes de connectivité, d'accessibilité et de résolution de nom. Utilisée sans paramètre, la commande Ping affiche l'aide.

Notes: sous l'invite de commande windows (**cmd**), pour obtenir un descriptif d'une commande et les arguments possibles associés à cette commande:
« commande » /HELP ou **« commande » /?**

Quelques commandes réseaux

Lancer cmd.exe sous Windows (interpréteur de commande)

Vérifier le bon fonctionnement de la carte réseau

ping 127.0.0.1 (ou "localhost")

"127.0.0.1" est une adresse ip réservée pour dire qu'il s'agit de votre propre PC !

On peut faire un ping de toute les "machines" qui ont une adresse IP:

ping 134.59.51.200

Ici il s'agit d'une imprimante !

Serveur mails de l'université
ping hermes.unice.fr

Adresse IP de cette machine ?

Quelques commandes réseaux

DNS (Domain Name Server) permet de retrouver une adresse IP en fonction d'un nom d'ordinateur (ou nom de domaine) et vis-versa

En fait, c'est une base de données qui contient tout les couples : adresses IP <=> nom de domaines

Mis au point pour permettre aux internautes d'utiliser des noms plutot que des nombres pour accéder à un serveur (beaucoup plus facile à retenir et manipuler que des suites de chiffres).

Les serveurs DNS hébergent cette base de données, qui est la meme partout dans le monde (milliers de copies identiques). Commande la plus connu de DNS : nslookup , pour interroger le DNS

Exemples :

nslookup www.unice.fr

=> adresse IP : 134.59.204.1

http://134.59.204.9 <=> http://www.unice.fr

nslookup 217.160.168.152

=> nom de la machine : ircan.org

http://217.160.168.152 <=> http://www.ircan.org

Quelques commandes réseaux

Remarque : Au moins 1 serveur DNS doit etre configuré sur un PC qui accède à Internet. (Sous windows, dans panneau de configuration, paramètres réseaux, propriétés adresses IP)

Autres exemples, tester des ping et des nslookup sur les adresses suivantes :

* webmail.unice.fr
* 217.160.168.152
* www.ircan.org

Au passage, quel est l'adresse IP du serveur DNS configuré sur votre machine ?

Quelques commandes réseaux

Tracert : (=traceroute sous Linux)

Envoie des paquets vers la machine en question et affiche la route empruntée sur le réseau pour l'atteindre.

Pour chaque étape sont affichés:

- le nom de la passerelle/routeur ou plus généralement du "noeud"
- les temps de trajet pour 3 essais successifs
- la présence d'une étoile indique une passerelle qui n'a pas répondu : surcharge du réseau,

ou alors si le nom n'apparaît pas c'est une volonté de masqué les informations depuis ce noeud

Quelques commandes réseaux

Il peut exister un firewall (pare-feu) qui interdit de renvoyer un echo d'un ping : la machine est bien connectée mais ne réponds pas !

---

ping www.kek.jp

ping www.auckland.ac.nz

Ces machines sont situées au japon (.jp) et en Nouvelle Zélande.

Comparez les temps de réponses par rapport aux machines locales comme " webmail.unice.fr "

tracert webmail.unice.fr

tracert www.kek.jp

tracert www.auckland.ac.nz

Comparez les chemins entre vous.

Quelques commandes réseaux

ipconfig (=ifconfig sous unix)

Affiche toutes les valeurs de la configuration du réseau TCP/IP et DNS (Domain Name System) et eventuellemnt les parametres DHCP *.

Utilisé sans paramètres, ipconfig affiche l'adresse IP, le masque de sous-réseau et la passerelle par défaut de toutes les cartes.

* Note: DHCP (Dynamic Host Configuration Protocol) est un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration réseau, en particulier une adreses IP automatique

DHCP est activé par défaut sur les box ADSL.

Le but principal étant la simplification de l'administration d'un réseau.

- Tester "ipconfig" sur votre machine

Quelques commandes réseaux

netstat

Affiche les connexions TCP actives et les ports sur lesquels l'ordinateur écoute, il affiche aussi la table de routage IP et les statistiques Ethernet, IPv4 et IPv6 (pour les protocoles IP, ICMP, TCP et UDP). Utilisée sans paramètre, la commande Netstat affiche les connexions TCP actives.

Note: De nombreux programmes TCP/IP peuvent être exécutés simultanément sur Internet (vous pouvez par exemple ouvrir plusieurs navigateurs simultanément ou bien naviguer sur des pages HTML tout en téléchargeant un fichier par FTP). L'ordinateur doit pouvoir distinguer les différentes sources de données. Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse unique sur la machine, codée sur 16 bits: un port (la combinaison adresse **IP + port** est alors une adresse unique au monde, elle est appelée **socket**

Quelques commandes réseaux

route

Affiche et modifie les entrées dans la table de routage IP locale. Utilisée sans paramètres, la commande route permet d'afficher l'aide.

La table de routage est une table de correspondance entre l'adresse de la machine visée et le noeud suivant auquel le routeur doit délivrer le message.

En d'autres termes la table de routage est une liste d'adresses IP des voisins connectés à ce noeud et quel voisin doit faire le relais d'un paquet IP en transit.

Autres commandes: hostname, arp, net (user, send)...

Matériel réseau

Les constituants matériels d'un réseau local

Un réseau local est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels permettant d'interconnecter les ordinateurs sont les suivants :

La carte réseau: il s'agit d'une carte connectée sur la carte-mère de l'ordinateur et permettant de l'interfacer au support physique, c'est-à-dire au lignes physiques permettant de transmettre l'information

Le transceiver: il permet d'assurer la transformation des signaux circulant sur le support physique, en signaux logiques manipulables par la carte réseau, aussi bien à l'émission qu'à la réception. Généralement intégré à la carte réseau.

La prise: il s'agit de l'élément permettant de réaliser la jonction mécanique entre la carte réseau et le support physique (exemple prise RJ45)

Le support d'interconnexion: c'est le support (généralement filaire, c'est-à-dire sous forme de câble) permettant de relier les ordinateurs entre eux. Les principaux supports utilisés dans les réseaux locaux sont les suivants : supports filaires (le câble coaxial, la paire torsadée, la fibre optique, le CPL), les supports sans-fil (Wi-Fi, bluetooth,...).

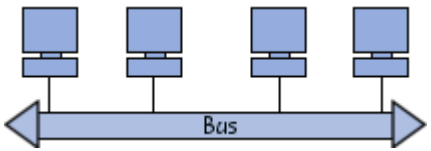
Matériel réseau

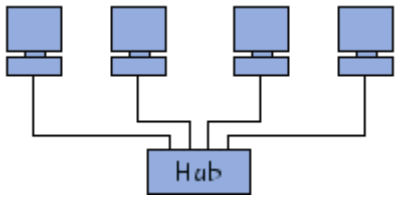
Topologies des réseaux locaux

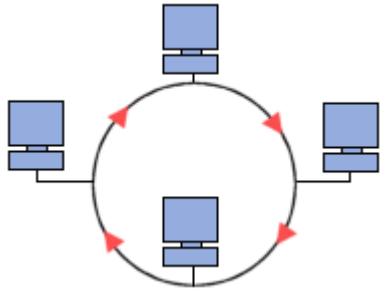
Les dispositifs matériels mis en oeuvre ne sont pas suffisants à l'utilisation du réseau local. En effet, il est nécessaire de définir une méthode d'accès standard entre les ordinateurs, afin que ceux-ci connaissent la manière de laquelle les ordinateurs échangent les informations, notamment dans le cas où plus de deux ordinateurs se partagent le support physique. Cette méthode d'accès est appelée **topologie logique.** La topologie logique est réalisée par un protocole d'accès. Les protocoles d'accès les plus utilisés sont :
Ethernet et **Token ring**

La façon de laquelle les ordinateurs sont interconnectés physiquement est appelée **topologie physique**. Les topologies physiques basiques sont :

la topologie **en bus** la topologie **en étoile** la topologie **en anneau**







La nécessité de l'interconnexion

Un réseau local sert à interconnecter les ordinateurs d'une organisation, toutefois une organisation comporte généralement plusieurs réseaux locaux, il est donc parfois indispensable de les relier entre eux. Dans ce cas, des équipements spécifiques sont nécessaires.

Lorsqu'il s'agit de deux réseaux de même type, il suffit de faire passer les données (trames) de l'un sur l'autre. Dans le cas contraire, c'est-à-dire lorsque les deux réseaux utilisent des protocoles différents, il est indispensable de procéder à une conversion de protocole avant de transférer les trames. Ainsi, les équipements à mettre en oeuvre sont différents selon la configuration face à laquelle on se trouve.

Matériel réseau

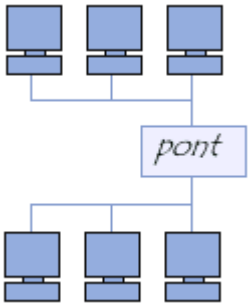
Les équipements d'interconnexion

Les principaux équipements matériels mis en place dans les réseaux locaux sont :

Les répéteurs, permettant de régénérer un signal

Les concentrateurs (hubs), permettant de connecter entre eux plusieurs hôtes

Les ponts (bridges), permettant de relier des réseaux locaux de même type



Les commutateurs (switches) permettant de relier divers éléments tout en segmentant le

Les passerelles (gateways), permettant de relier des réseaux locaux de types différents

Les routeurs, permettant de relier de nombreux réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de la façon optimale

Les B-routeurs, associant les fonctionnalités d'un routeur et d'un pont

Les fournisseurs d’accès internet

Pourquoi un FAI ?

Note: Fournisseur d'accès à Internet = FAI = provider = ISP (Internet Service Provider).
C'est un service (la plupart du temps payant) qui vous permet de vous connecter à Internet...

A moins d'avoir une ligne spécialisée (autre que la ligne téléphonique, type cable optique), vous ne pouvez pas vous connecter directement à internet par votre ligne de téléphone. En effet, la ligne de téléphone n'a pas été prévue à cet effet :

• elle est originalement prévue pour transporter des "voix", c'est-à-dire une modulation de fréquence de l'ordre du timbre de la voix

• les serveurs téléphoniques ne savent initialiser une communication qu'à partir d'un numéro de téléphone et/ ou login + mot de passe

• à moins d'avoir recours à un service spécial, il n'est généralement pas possible d'avoir une communication entre plus de deux points...

Ainsi, le fournisseur d'accès internet est un intermédiaire (connecté à internet par des lignes spécialisées) qui va vous procurer un accès à internet par son biais, grâce à votre modem (=box) qui permet d'établir une connexion.

Les fournisseurs d’accès internet

Comment le FAI vous connecte-t-il à Internet ?

Lorsque vous vous connectez à Internet par l'intermédiaire de votre fournisseur d'accès, il s'établit une communication entre vous et le FAI grâce à un protocole simple: le PPP (Point to Point Protocol), un protocole permettant de mettre en communication deux ordinateurs distants sans que ceux-ci ne possèdent d'adresse IP.
En effet votre ordinateur ne possède pas d'adresse IP. Cette adresse IP est toutefois une condition nécessaire pour pouvoir aller sur Internet, car le protocole utilisé sur Internet est le protocole TCP/IP, qui permet de faire communiquer un nombre très important d'ordinateurs repérés par ces adresses.

Ainsi, la communication entre vous et le fournisseur s'établit selon le protocole PPP, qui se caractérise par :

- un appel téléphonique / Dsl / fibre
- une initialisation de la communication
- la vérification du nom d'utilisateur (login ou userid)
- la vérification du mot de passe (password)

=> C'est étape sont par exemple intialisées lorsqu'on redémarre sa « box »

Les fournisseurs d’accès internet

Les différences entre les FAI

Une fois que vous êtes "connecté", le fournisseur d'accès vous prête une adresse IP que vous garderez pendant toute la durée de la connexion à internet. Celle-ci n'est toutefois pas fixe, car dès la connexion suivante le fournisseur vous donnera une de ses adresses libres (donc différente car il peut en posséder, selon sa capacité, plusieurs centaines de milliers...).
Votre connexion est donc une connexion par procuration car c'est votre fournisseur qui envoie toutes les requêtes que vous faites, et c'est lui qui reçoit les pages que vous demandez et qui vous les réexpédie.

Dans certains cas particuliers, le FAI peut vous octroyer une adresse IP fixe (en général, les lignes dégroupées) .

Les FAI traditionnels ne concernent en général pas les grands organismes (universités, centres de recherche). Les adresses IP sont fixes dans la plupart des cas.

Les fournisseurs d’accès internet

Les différences entre les FAI

Le choix d'un FAI se fait selon de nombreux critères dont le nombre de services offerts et la qualité de ces services :

• La couverture: certains FAI ne proposent une couverture très haut débit que dans les grandes villes (ADSL, cable fibre).

• La bande passante: c'est le débit total que propose le FAI. Cette bande passante se divise par le nombre d'abonnés, ainsi plus le nombre d'abonnés augmente plus celle-ci devient petite. Dépends du lieu géographique.

• La latence, le débit montant et descendant

• Le prix: celui-ci dépend du FAI et du type de formule choisie (triplay, etc.).

• Les éventuels quotas temps ou quotas transfert données :

- illimité en général si ADSL / Cable (mais peut changer...)
- limité si tél portable / clée 3G ou 4G (fair-use) ou accès satellite.

Les fournisseurs d'accès internet

ACERP (www.arcep.fr) - Autorité de régulation des communications électroniques et des postes

=> observatoire sur la "qualité de l'accès aux services fixes" : rapport traite des débits, de la latence et de la qualité de navigation effective chez chaque opérateur. L'organisme teste :

• Le débit descendant avec une mire proche (un site situé en France chez un hébergeur disposant d'une bonne interconnexion avec tous les opérateurs testés) + le débit descendant avec une mire lointaine (à l'étranger, pour mesurer "le ressenti de l'utilisateur lorsqu'il utilise des services hébergés plus loin du réseau de son opérateur")

• le débit montant avec une mire proche + le débit montant avec une mire lointaine.

L'Autorité précise en outre que "les débits mesurés sont des débits moyens IP, ce qui signifie qu'il s'agit d'une vitesse moyenne (et non d'une vitesse maximale) réellement disponible pour l'utilisateur".

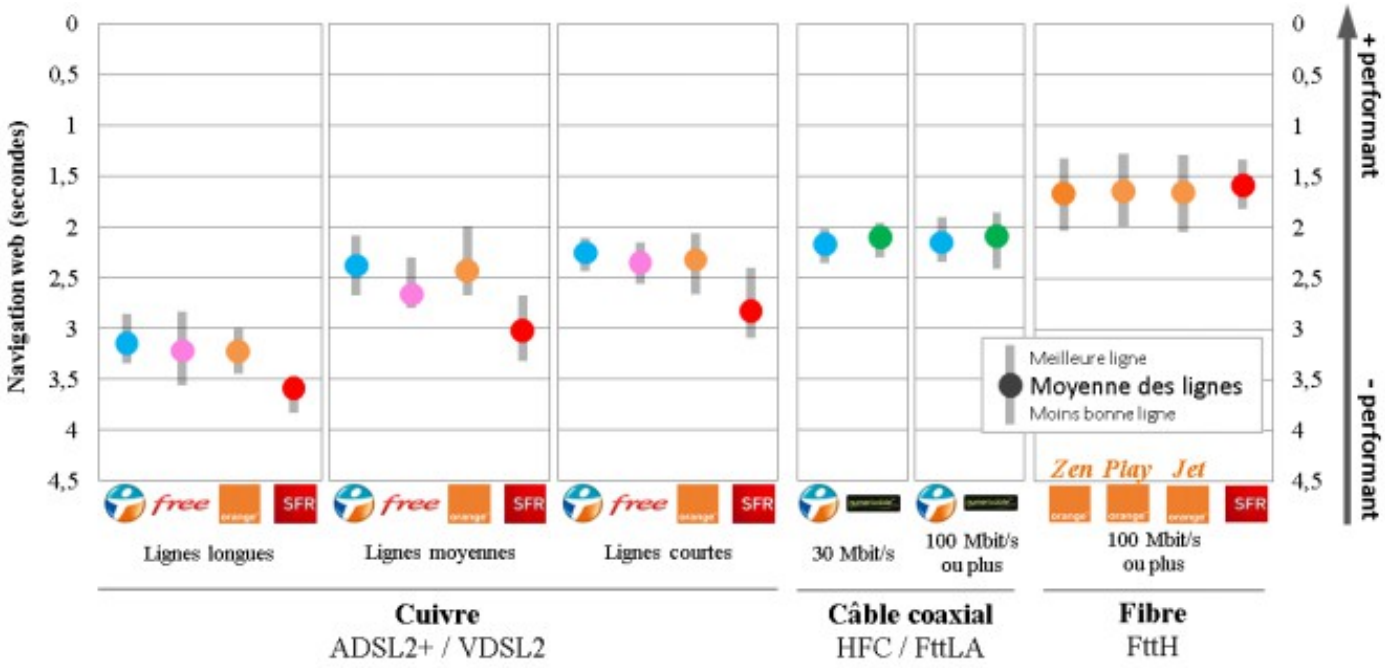


Figure 12 – Usage « navigation web ».

Les fournisseurs d’accès internet

• Autres éléments à prendre en compte:

- Le service technique: c'est une équipe chargée de répondre à vos problèmes techniques (appelé aussi hot-line ou bien service clientèle). Les FAI font généralement payer ce type de service.

- Les services annexes : nombre d'adresses e-mail, espace mis à disposition pour la création d'une page perso (HTML), etc...

- Réputation du FAI...

• Quelques sites pour avoir plus d'infos:

-www.01net.com, http://www.dslvalley.com, http://www.testadsl.net/
permet de comparer les différentes offres des opérateurs.

- www.grenouille.com est un site utile pour connaître la météo du net, c'est-à-dire les débits observés en temps réel sur les lignes des fournisseurs d'accès haut débit.

L'architecture client/serveur

Présentation de l'architecture d'un système client/serveur

De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc.

Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes. On parle ainsi de client (client FTP, client de messagerie, etc.) lorsque l'on désigne un programme tournant sur une machine cliente, capable de traiter des informations qu'il récupère auprès d'un serveur (dans le cas du client FTP il s'agit de fichiers, tandis que pour le client de messagerie il s'agit de courrier électronique).

L'architecture client/serveur

Avantages de l'architecture client/serveur

Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :

• des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction

• une meilleure sécurité : car le nombre de points d'entrée permettant l'accès aux données est moins important

• une administration au niveau serveur : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés

• un réseau évolutif : grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure

Inconvénients de l'architecture client/serveur

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

• un coût élevé dû à la technicité du serveur

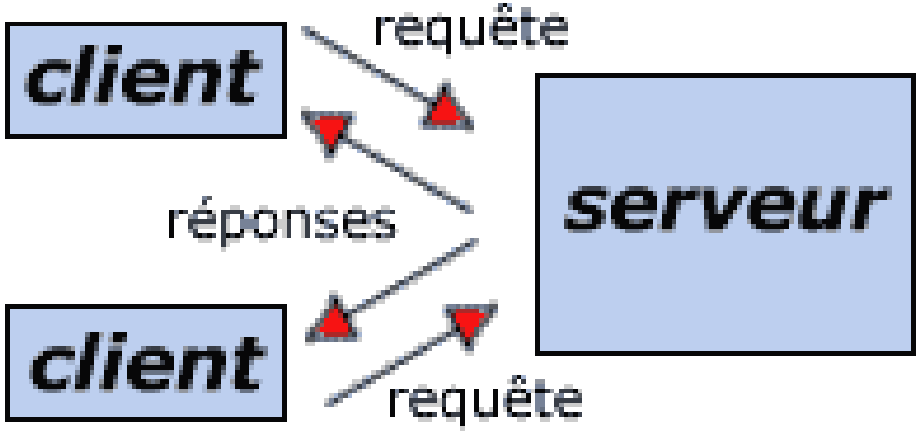
• un maillon faible : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce aux différents systèmes RAID)

Fonctionnement d'un système client/serveur

Un système client/serveur fonctionne selon le schéma suivant :

• Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur

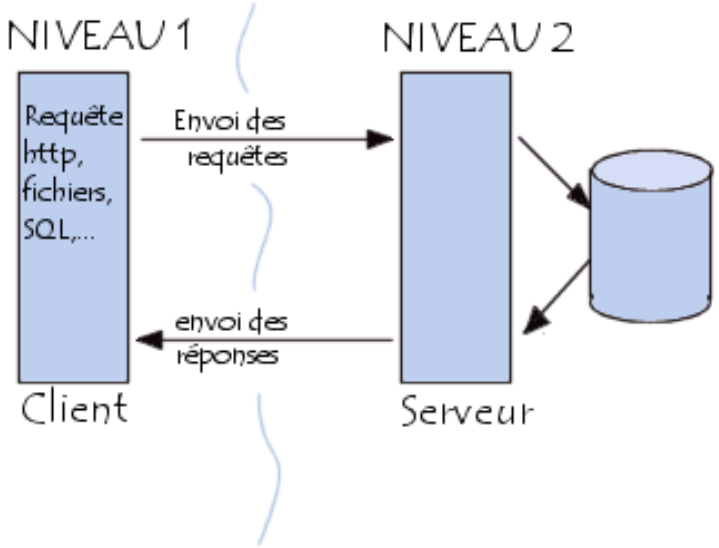
• Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port



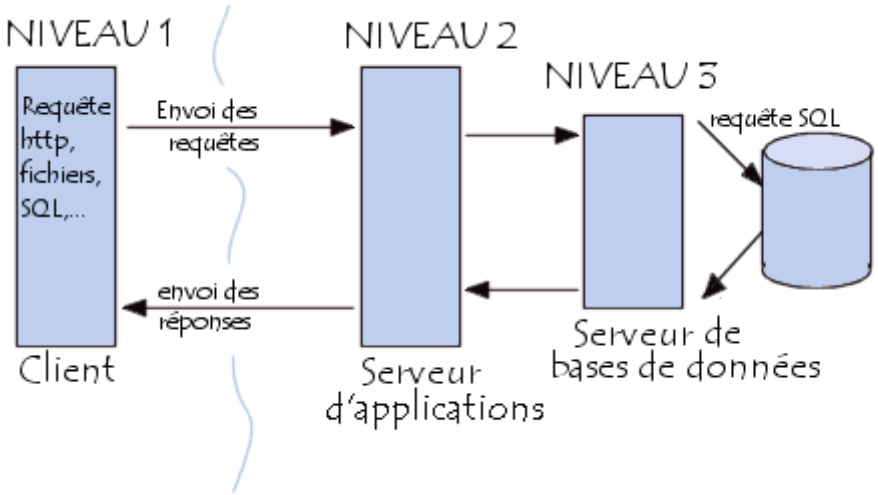
L'architecture client/serveur

Présentation de l'architecture à plusieurs niveaux

L'architecture à deux niveaux (aussi appelée architecture 2-tier, tier signifiant rangée en anglais) caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources. Cela signifie que le serveur ne fait pas appel à une autre application afin de fournir une partie du service.



L'architecture à 3 niveaux (appelée architecture 3-tier), il existe un niveau intermédiaire, c'est-à-dire que l'on a généralement une architecture partagée entre :
Un client (l'ordinateur demandeur de ressources), le serveur d'application (appelé également middleware), chargé de fournir la ressource mais faisant appel à un autre serveur: le serveur de données, fournissant au serveur d'application les données dont il a besoin.
Il peut y avoir plusieurs serveurs de données



Architecture client/serveur : Exemple 1 – FTP

Protocole et serveur FTP

Le protocole FTP (File Transfer Protocol) est un protocole de communication dédié à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers depuis ou vers un autre ordinateur du réseau, d'administrer un site web, ou encore de supprimer ou modifier des fichiers sur cet ordinateur.

En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend publique une arborescence de fichiers similaire à un système de fichiers Unix. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande).

FTP est très souvent utilisé en Sciences notamment pour télécharger de gros fichiers rapidement (exemple: données d'études, résultats d'expériences, séquences nucléotidiques, ...)
C'est aussi le protocole utilisé lorsqu'on a créé un site et qu'on veut le faire héberger : vos fichiers sont envoyés de votre ordinateur vers le serveur web de l'hébergeur par FTP

Note: SFTP est identique au FTP mais sécurisé (les données qui transitent sur le réseau sont cryptées). SFTP est peu utilisé.

Architecture client/serveur : Exemple 1 – client FTP

Comment utiliser FTP comme client ?

• Par un navigateur web

La plupart des navigateurs récents autorisent les connexions FTP en utilisant une URL de type :
ftp://nom_d_utilisateur:mot_de_passe@nom_du_serveur:port_ftp
Par sécurité, il est conseillé de ne pas préciser le mot de passe, le serveur le demandera. Cela évite de le laisser visible en clair ou réutilisable. La partie port_ftp est optionnelle. S'il est omis le port par défaut (21) sera utilisé.
FTP par un navigateur est souvent très limité et n'autorise en général que la lecture de fichiers sur le serveur

• Par la commande « ftp »

La commande « ftp » (suivie des arguments de connexion) est accessible sur tous les systèmes d'exploitation. Toutes les fonctions sont disponibles mais l'utilisation de ftp en ligne de commande est peu pratique

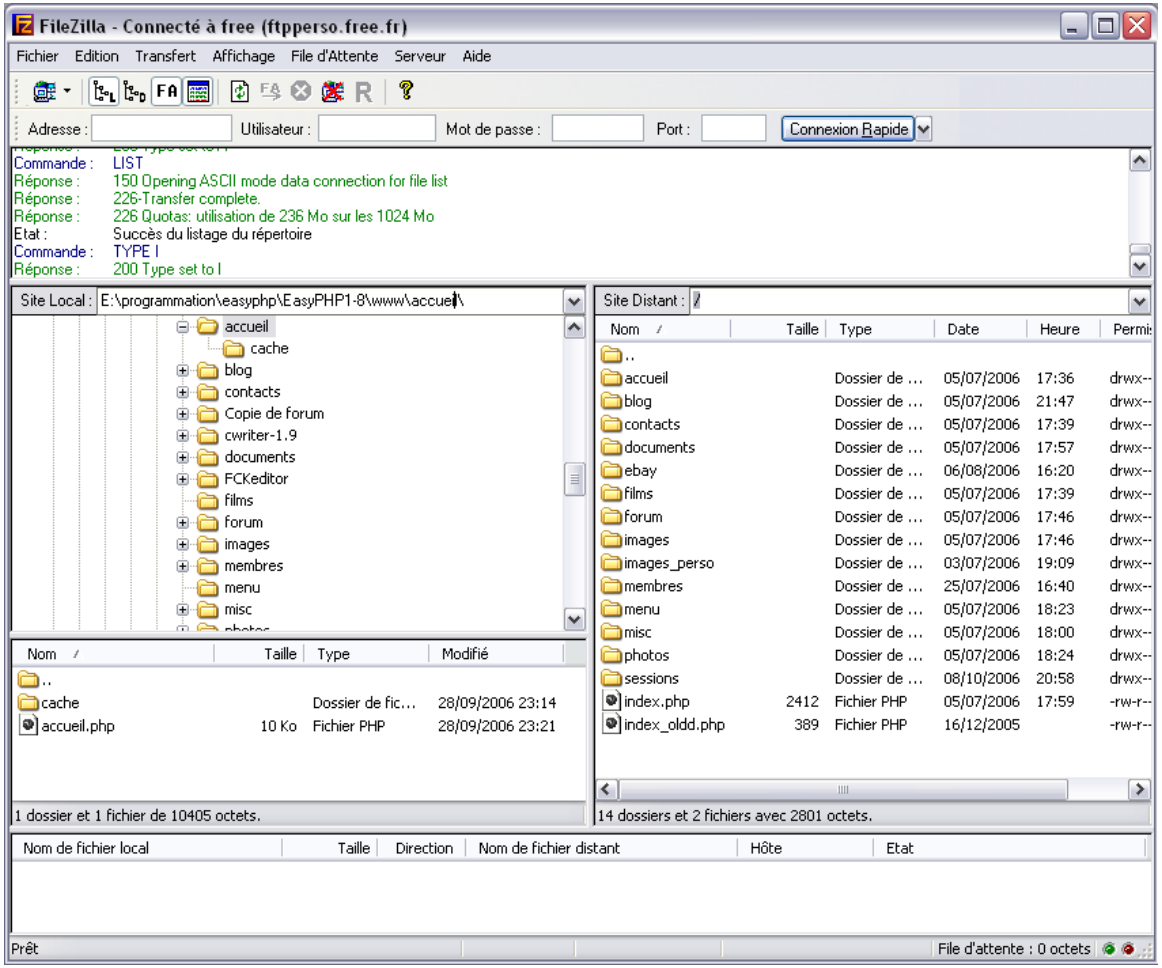
Architecture client/serveur : Exemple 1 – client FTP

Comment utiliser FTP comme client ?

• **Logiciel client FTP**

Il existe plusieurs logiciels avec une interface graphique permettant de se connecter à un serveur FTP pour télécharger ou pour copier des fichiers. Certains logiciels tels que CuteFTP (Windows) sont payants; d'autres, tels que FileZilla (Windows), Cyberduck (MacOSX) ou gftp (Linux), tout aussi pratiques et efficaces, sont gratuits et libres.

Filezilla est téléchargeable sur filezilla.sourceforge.net



Architecture client/serveur : Exemple 1 – client FTP

Exemple d'utilisation d'un client FTP

- Télécharger et installer filezilla

- Ouvrir filezilla et aller sur le serveur ftp du NCBI (ftp.ncbi.nih.gov)

L'accés se fait de manière « anonyme » c'est à dire que des identifiants par défaut sont utilisés (login: « anonymous », password: « anonymous »).

Si le serveur est configuré pour accepter les clients « anonymes » alors vous aurez accés aux fichiers du serveur (en lecture seule cependant).

Notez que si vous n'entrez pas d'identifiants dans filezilla, la connexion se fait en « anonymous » par défaut.

A gauche vous avez l'arborescence de votre ordinateur, à droite celle du serveur.

- Accéder au répertoire « genomes » et télécharger sur votre machine un fichier de petite taille (le « README » par exemple).

- Fermer la connexion (la connexion se ferme en général automatiquement au bout d'un certain temps d'inactivité)

Architecture client/serveur : Exemple 2 – VNC

VNC = Virtual Network Computing

Il s'agit de prendre très facilement le contrôle d'un PC à distance en utilisant un programme.

Par exemple, si vous souhaitez dépanner un ami, prenez le contrôle de son PC et faîte les modifications à sa place, en direct, comme si vous êtiez sur votre propre PC !

Exemple avec Real VNC: gratuit (open source) et multi plateformes.

http://www.pcanywhere.com/

ou : www.tightvnc.com

ou : www.teamviewer.com

Architecture client/serveur : Exemple 2 – VNC

Prise de contrôle à distance avec Real VNC

Cette méthode permet d'afficher dans une fenêtre « Windows » de votre ordinateur (appelé client), le bureau d'un ordinateur distant (appelé serveur).

Ceci peut être utile pour plusieurs raisons :

- besoin d'accéder à 2 PC en même temps sans avoir d'écran supplémentaire et donc sans avoir besoin de jongler avec votre prise VGA

- Utiliser un ordinateur qui n'est pas à coté de l'utilisateur, dans la pièce à coté ou à l'autre bout du monde

Dans le cas d'un réseau local, seuls les fichiers et imprimantes sont partagés ce qui peut être insuffisant (la prise de contrôle permet également de partager les applications)

Il est possible de contrôler des machines qui ne sont pas sous Windows et ceci sans utiliser les outils Microsoft d'utilisation à distance

Dans les entreprises, le dépannage peut se faire à distance.

Architecture client/serveur : Exemple 2 – VNC

Real VNC

Ce logiciel permet donc de réaliser ces manipulations, il a été créé par l'université de Cambridge en partenariat avec AT&T.

Ses avantages :
Gratuit,
Léger,
Open source,
Multi plateformes :
Linux (sur x86)
Unix (sources non compilées)
Solaris (SPARC)
Windows 9x/NT/2000/XP/2003
Macintosh (Beta)
DEC Alpha OSF1 3.2
Windows CE 2.x (Beta)
En français.

Notez qu'il existe de nombreux autres logiciels permettant de réaliser la même chose payant ou gratuit

Téléchargez : Real VNC (pour Windows) et l'installer

Architecture client/serveur : Exemple 2 – VNC

Ce logiciel se décompose en deux composants : le serveur et le client

Configurer le serveur

Utilisez VNC en tant que service donne la possibilité de prendre le contrôle d'une machine à distance même si l'utilisateur n'a pas démarre le serveur.

-> le serveur démarre automatiquement en même temps que le PC

Il doit être exécuté sur le poste que l'on souhaite piloter à distance.

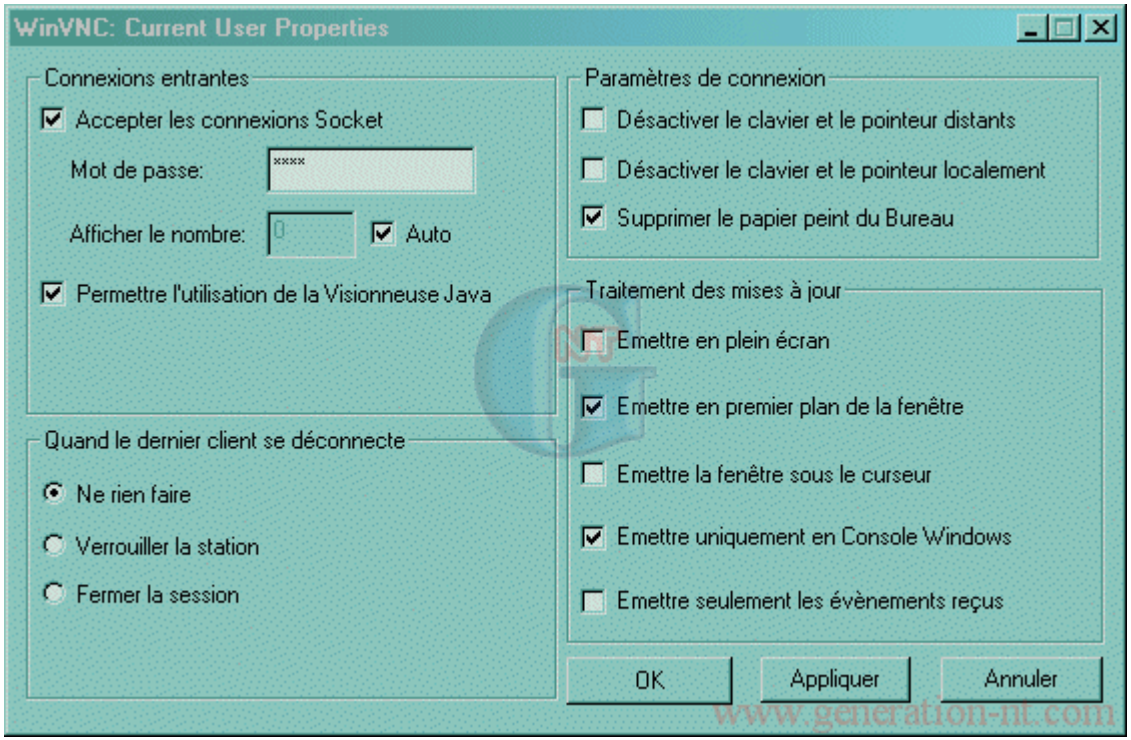
Si le serveur ne démarre pas automatiquement en tant que service, le faire lancer comme « applications » au démarrage par windows.
Pour ce faire, copiez le raccourci intitulé « Run VNC Server » dans le dossier « démarrage » du menu démarrer..

On obtient dans la barre de notification des tâches ceci : 

L'IP affichée lorsque l'on passe le curseur sur l'icône, correspond à l'adresse de l'ordinateur sur le réseau local.

Architecture client/serveur : Exemple 2 – VNC

Effectuez un clic droit sur l'icône puis choisissez l'option "Propriétés":



La première chose à faire est de choisir un mot de passe afin de sécuriser la connexion du client.

Les options qui sont proposées dans la fenêtre ci-dessus conviennent à la quasi-totalité des utilisations.

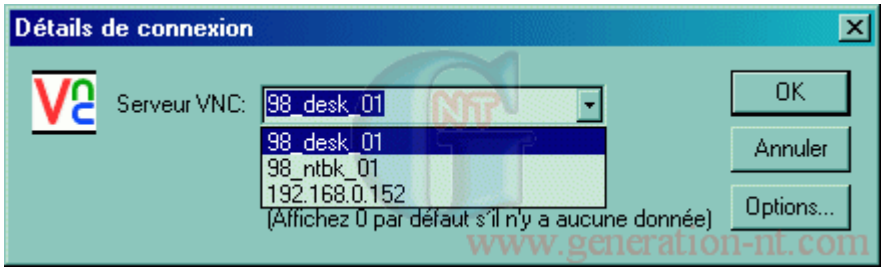
Architecture client/serveur : Exemple 2 – VNC

Le client

Il va permettre le contrôle à distance des ordinateurs exécutant le serveur.

Pour lancer le client, il faut ouvrir le menu démarrer puis "realVNC" et choisir "Run VNC Viewer...".

Choisissez l'adresse ip du serveur



Dans le champ "Serveur VNC", saisir soit:
- Le nom du PC
- Son adresse IP

Puis le mot de passe (celui configuré sur le serveur)

L'icône de VNC serveur est devenue noire, signe d'une prise de contrôle. Vous pouvez maintenant gérer votre ordinateur distant comme un programme sur votre ordinateur local.

Pour interrompre la prise de contrôle, il faut soit :
Fermer la fenêtre du client,
Faire un clic droit sur l'icône du serveur et choisir "Fermer VNC".

Architecture client/serveur : Exemple 3 – serveur FTP

Il existe plusieurs serveurs FTP gratuits et simples.

Exemple avec **TYPSOFT**: http://fr.typsoft.com/

Télécharger et installer le programme.

Démarrer le serveur.

Dès la première utilisation, le serveur utilise le port 21, qui est le port utilisé par défaut pour les serveur FTP.

Architecture client/serveur : Exemple 3 – serveur FTP

Configuration

Cette opération n'est pas obligatoire étant donné que la configuration par défaut est tout à fait acceptable. Cependant, il vaut mieux choisir sa propre configuration

Architecture client/serveur : Exemple 3 – serveur FTP

Configuration des comptes utilisateurs - Compte anonyme - Compte par défaut

Il existe un compte par défaut, le compte anonyme, qui permet aux utilisateurs de ne pas avoir besoin de nom d'utilisateur, ni de mot de passe pour se connecter sur le serveur. Cela peut présenter quelques avantages mais aussi quelques inconvénients.

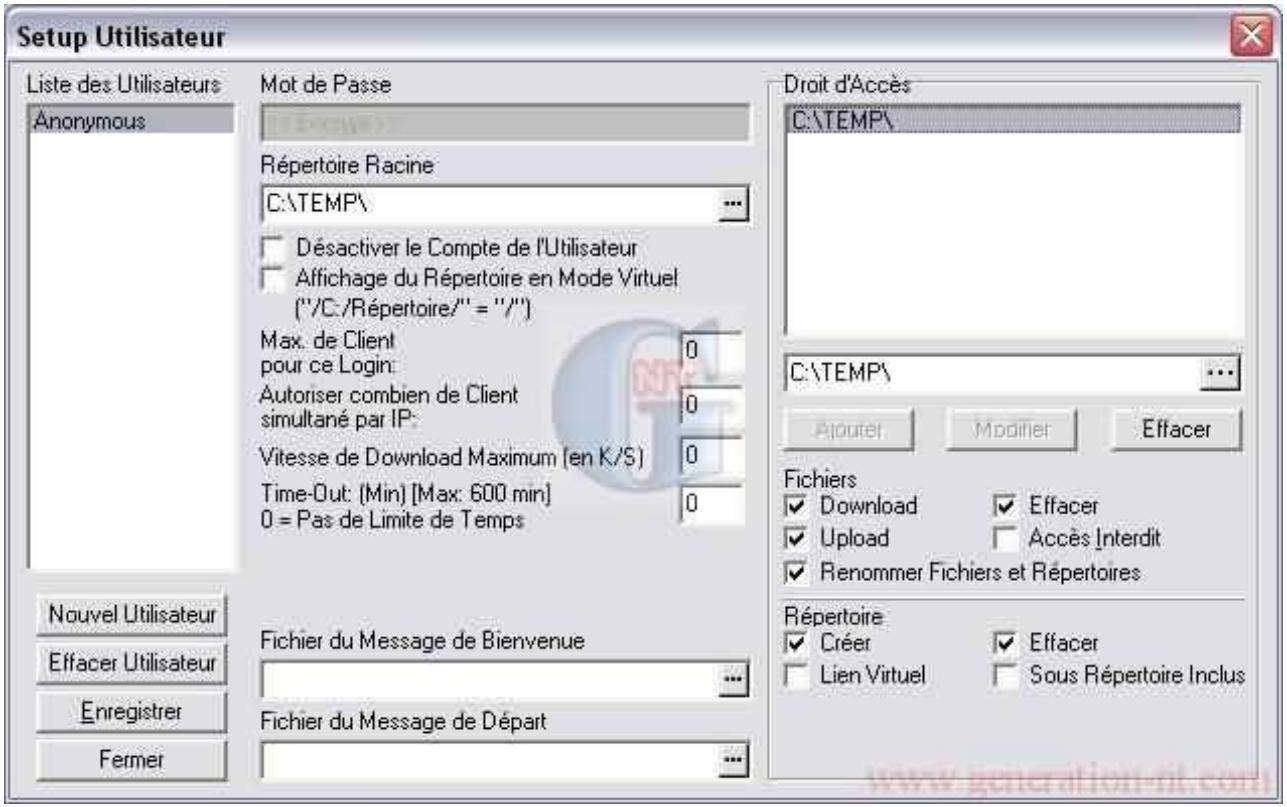
Cela permet, dans le cadre d'un usage personnel, d'etre plus simple et plus rapide. Vous n'avez pas besoin de configurer de comptes particuliers.

Mais cela permet aussi à n'importe qui de se connecter sur votre ordinateur pour faire on ne sait quoi.

Donc cela peut présenter des intérêts, mais je vous conseille malgré tout de cocher la case "Désactiver le compte de l'utilisateur" et d'enregistrer, mais là encore tout dépend de l'utilisation qui est destinée au serveur FTP...

Architecture client/serveur : Exemple 3 – serveur FTP

Depuis la fenêtre principale de FTP Server, dans le menu "Configuration" cliquez sur "Utilisateurs".



Pour créer un nouvel utilisateur, cliquez sur le bouton "Nouvel Utilisateur" et vous obtiendrez une fenêtre où vous pourrez saisir le nom de l'utilisateur.
Refaites cette opération autant de fois que vous voulez d'utilisateurs.

Il est possible de personnaliser la configuration en fonction de chaque utilisateur, pour cela sélectionnez un utilisateur dans la liste de gauche et indiquez les paramètres individuels :

Architecture client/serveur : Exemple 3 – serveur FTP

* Mot de passe : Permet de définir le mot de passe que l'utilisateur concerné devra utiliser pour pouvoir se connecter.

* Répertoire racine : Répertoire par défaut de l'utilisateur concerné, quand il se connectera sur votre serveur, il sera automatiquement placé dans ce répertoire.

* Désactiver le compte utilisateur : L'utilisation de ce compte sera impossible si cette case est cochée.

* Affichage du répertoire en mode virtuel : Si cette case est cochée, l'utilisateur connecté n'aura accès qu'à un chemin d'accès virtuel : si par exemple, vous avez un utilisateur dont le chemin d'accès du répertoire racine est C:\FTP\Utilisateur, l'utilisateur en question ne verra que /Utilisateur.

* Max. de client pour ce login : Nombre maximum d'utilisateurs pouvant se connecter sous un même nom d'utilisateur.

* Autoriser combien de client simultané par IP : C'est le nombre d'utilisateurs qui pourront se connecter sur votre serveur depuis un seul ordinateur, ou le nombre de sessions qu'un même utilisateur a le droit de lancer.

* Vitesse de download maximum : C'est le taux de transfert maximum que vous autorisez à l'utilisateur concerné, cela peut avoir l'avantage d'équilibrer les débits s'il y a plusieurs utilisateurs en même temps sur votre serveur, ou tout simplement de privilégier un utilisateur.

* Time-Out : Durée à partir de laquelle l'utilisateur sera déconnecté sur le serveur s'il n'a aucune activité.

* Fichier du message de Bienvenue : Message de bienvenue personnalisé à l'utilisateur concerné.

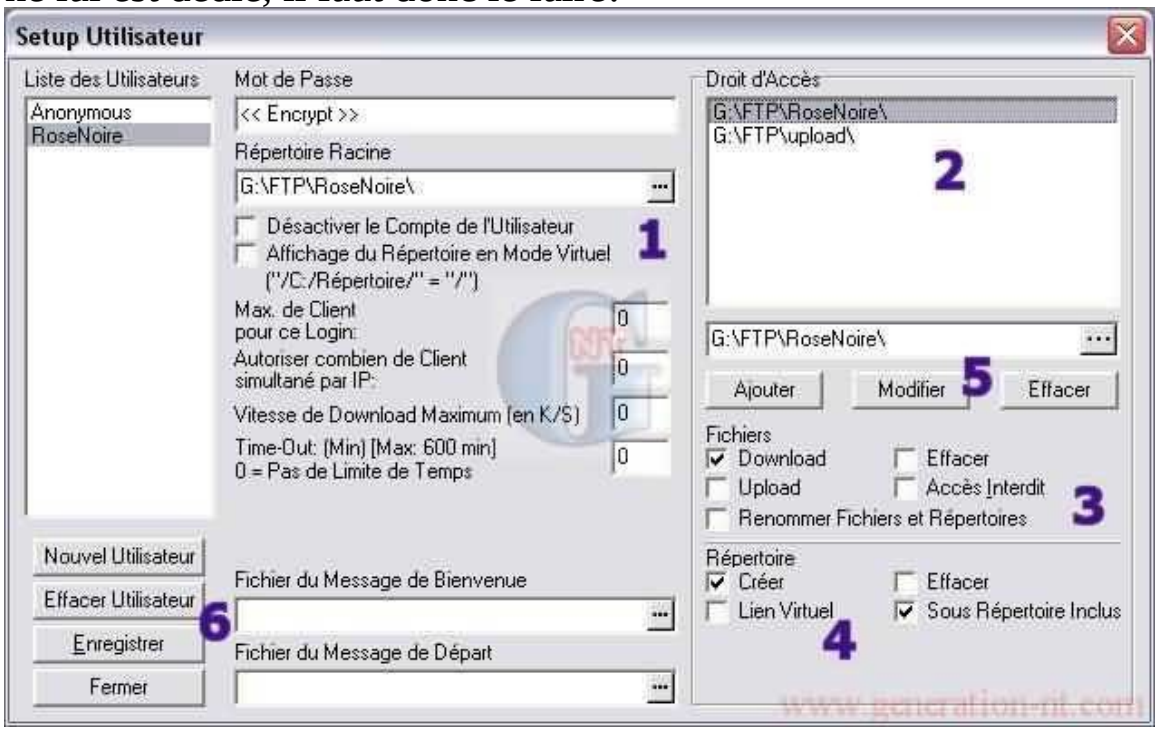
* Fichier du message de Départ : Message de départ personnalisé à l'utilisateur concerné.

Remarque : la valeur "0" signifie qu'il n'y a aucune limite, que ce soit en bande passante ou en nombre d'utilisateurs.

Architecture client/serveur : Exemple 3 – serveur FTP

Attribuer les droits aux utilisateurs

Lorqu'un nouvel utilisateur est créé, aucun répertoire ne lui est dédié, il faut donc le faire.



1 - Cliquez sur ... et sélectionnez le répertoire de votre disque dur que vous souhaitez dédier à cet utilisateur.

2 - Sélectionnez ce répertoire dans la liste à droite.

3 - Appliquez les droits que vous voulez pour les fichiers :

Download : Donne les droits au téléchargement de fichiers.
Upload : Donne les droits d'envoi de fichiers.
Effacer : Donne le droit d'effacer des fichiers.
Accès Interdit : Interdit l'accès au répertoire.
Renommer fichiers et répertoires : Donne le droit de renommer des fichiers ou des répertoires.

4 - Appliquez les droits que vous voulez pour les répertoires :

Créer : Donne le droit de créer des répertoires.
Effacer : Donne le droit d'effacer un répertoire.
Sous-répertoire inclus : Donne les mêmes droits aux sous-répertoires.

5 - Cliquez sur Modifier pour valider vos modifications

6 - Cliquez sur Enregistrer pour enregistrer vos modifications, attention si vous changez d'utilisateur ou fermez la fenêtre pendant les modifications, celles-ci seront perdues !

Architecture client/serveur : Exemple 3 – serveur FTP

Conclusion

Vous avez maintenant terminé la configuration de votre serveur FTP et il est possible d'y accéder par l'adresse du serveur;

Vous pouvez utiliser un client graphique comme filezilla