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

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 ordinateurs sont reliés entre eux.

- Données partagées : fichiers accessibles sur les serveurs du réseau

Imprimantes et autres périphériques partagés : fichiers, imprimantes ou autres éléments utilisés par les usagers du réseau

- Ressources diverses : autres ressources fournies par le serveur

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 (pour un réseau ethernet par exemple) et 1 Gbps (en FDDI ou Gigabit Ethernet par exemple). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs.

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 réseau 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) à des débits importants. Ainsi un MAN permet à deux noeuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

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 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

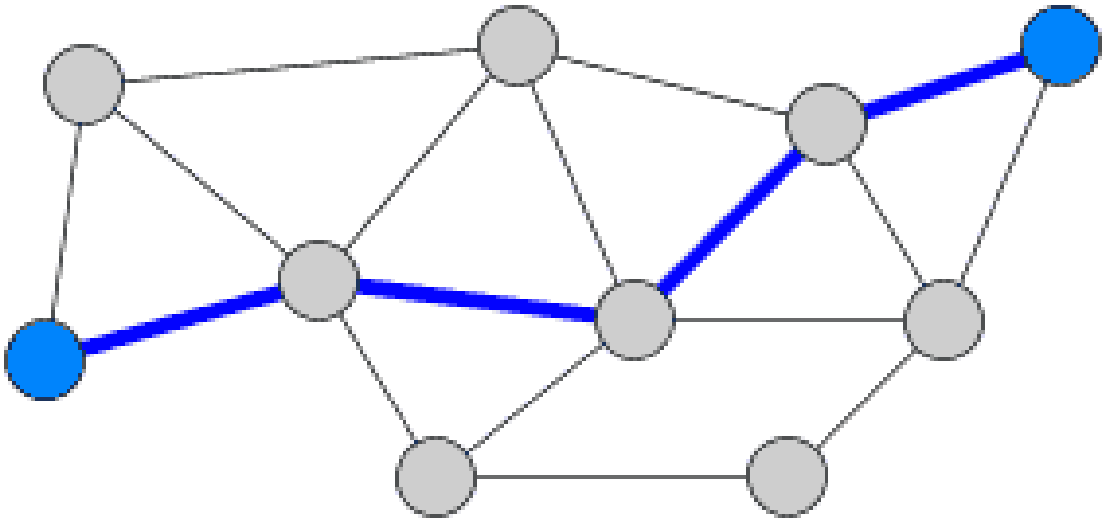
Internet est la suite du réseau militaire américain ARPANET.

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).

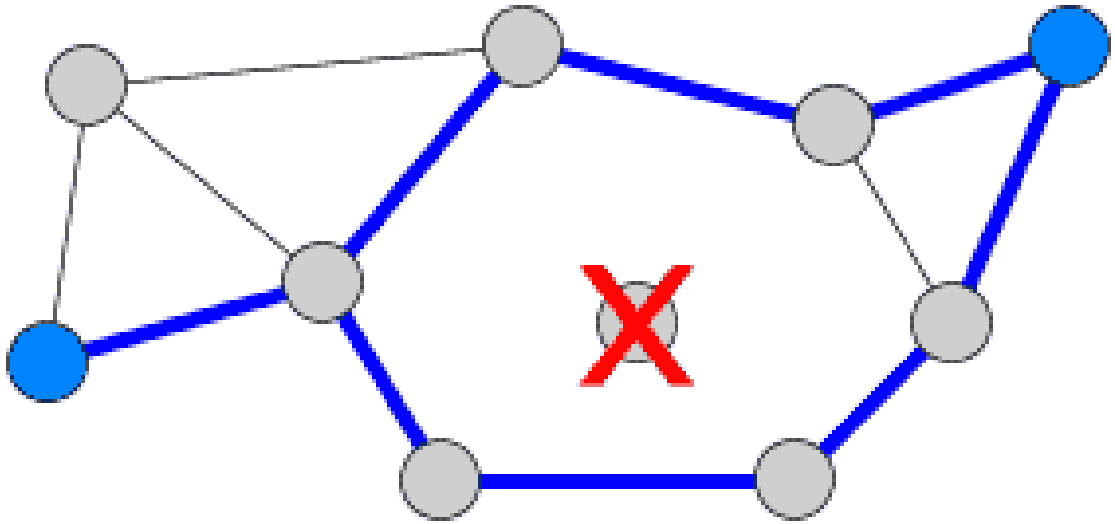
Internet a donc été conçu dès l'origine comme une toile d'araignée, d'où son nom anglais web (qui veut dire tissage et toile d'araignée).

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 prête une le temps de 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.

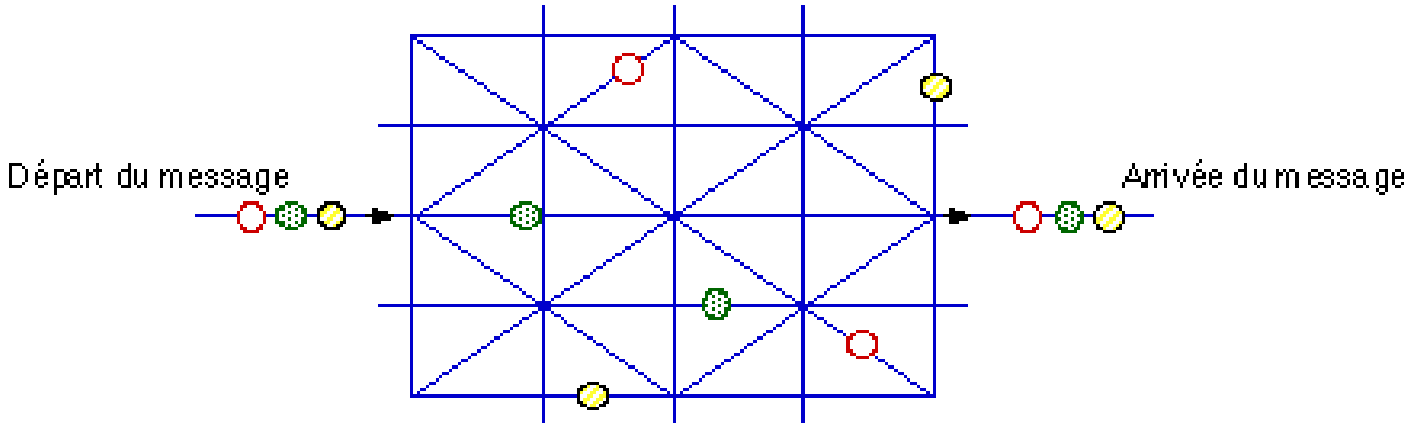
Internet utilise un système international d'adresses qui permet d'envoyer un message ou un fichier sans ambiguïté à un correspondant connecté.

Chaque ordinateur a une adresse unique.

-> Principe du réseau décentralisé et redondant.

Le Réseau Internet

Le transfert de données



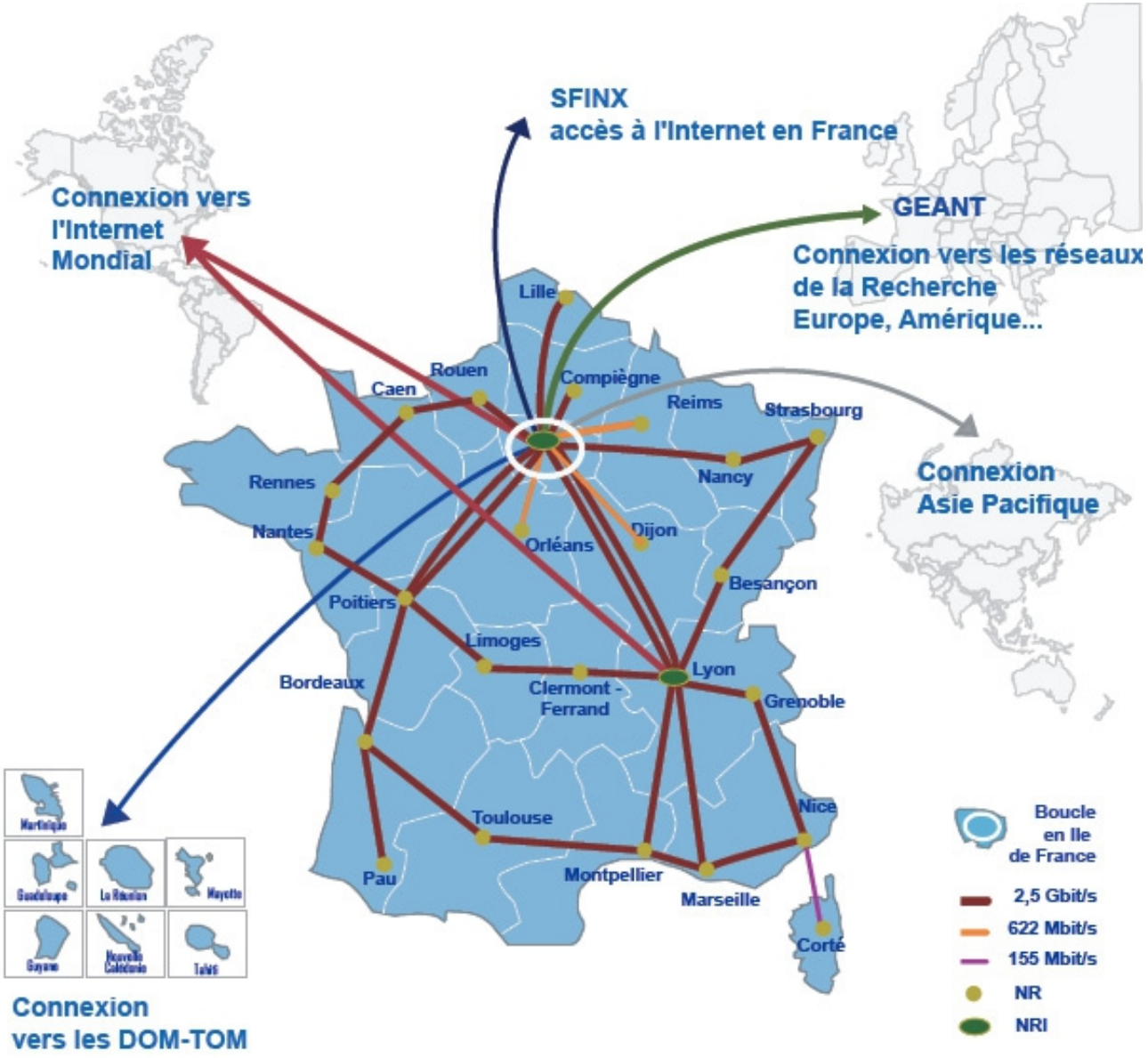
Chaque ordinateur constitue un nœud du réseau. Il est identifié par une adresse IP (Internet Protocole) qui est son identificateur.

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



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.

TCP/IP : Transmission Control Protocol / Internet Protocol

Défini la norme de communication, (en fait un ensemble de protocoles) des ordinateurs reliés à Internet.

Va contenir les protocoles HTTP, FTP, SMTP, …

Adresse IP : utilise des numéros de 32 bits que l'on écrit sous la forme de 4 numéros allant de 0 à 255 (4 fois 8 bits)

xxx.xxx.xxx.xxx

Donc environ 4 milliards d'adresses différentes

• **DNS** permet de retrouver une adresse IP en fonction d'un nom d'ordinateur (un peu comme un annuaire).

• **FTP** sert à transporter des fichiers d'un ordinateur à l'autre.

• **IRC** permet de créer des «salons» de discussion en direct.

• **ICQ** permet de savoir si quelqu'un est en ligne et de dialoguer avec lui.

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

• **P2P** permettent de partager des fichiers à grande échelle.

• **NNTP** permet d'accéder à des forums de discussion sur des milliers de sujets différents.

• **SSH** permet d'avoir un accès sécurisé à des ordinateurs distants.

• **SMTP** permet d'envoyer des emails, et le protocole POP3 de les recevoir.

DNS : Domain Name Server : système de nom de domaine ou système d'affectation de nom.

Système distribué de bases de données et de serveurs qui assure la traduction des noms de domaine utilisés par les internautes en numéros IP utilisables par les ordinateurs.

Mis au point pour permettre aux internautes d'utiliser des noms dans la rédaction des adresses (beaucoup plus facile à manipuler que des suites de chiffres).

Exemples :

nom : www.unice.fr

-> IP : 134.59.1.71

nom : bach.ebgm.jussieu.fr

-> IP : 134.157.50.1

FTP: protocole définissant les règles de transfert des fichiers par Internet. Lorsqu'un utilisateur télécharge un fichier par ftp, il le recopie de l'ordinateur distant sur le sien (ou l'inverse).

TELNET : protocole standard permettant l'interfaçage de terminaux et d'applications à travers Internet.

Ce protocole fournit les règles de bases pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un ordinateur distant (coté serveur)

Attention: Protocoles de transfert non sûrs, c'est-à-dire que les données circulent en clair sur le réseau.

La messagerie électronique

- Le courrier électronique est considéré avec le web comme étant le service le plus utilisé sur Internet. Ainsi la suite de protocoles TCP/IP offre une panoplie de protocoles permettant de gérer facilement le routage du courrier sur le réseau.

- Le protocole **SMTP** (Simple Mail Transfer Protocol, traduisez Protocole Simple de Transfert de Courrier) est le protocole standard permettant de transférer le courrier d'un serveur à un autre en connexion point à point.

  Il s'agit d'un protocole fonctionnant en mode connecté, encapsulé dans une trame TCP/IP. Le courrier est remis directement au serveur de courrier du destinataire. Le protocole SMTP fonctionne grâce à des commandes textuelles envoyées au serveur SMTP (par défaut sur le port 25). Chacune des commandes envoyées par le client (validée par la chaîne de caractères ASCII CR/LF, équivalent à un appui sur la touche entrée) est suivi d'une réponse du serveur SMTP composée d'un numéro et d'un message descriptif.

Exemple de commandes réseaux

Exemple du protocole **ICMP** (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs aux machines connectées. Etant donné le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire part de ces erreurs aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour signaler une erreur (appelé Delivery Problem).

Ping : teste la présence d'une machine sur le réseau. Compte le temps nécessaire pour aller de la machine où l'on se trouve à la machine appelée.

Exemple de commandes réseaux

Tracert : (traceroute) 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
- les temps de trajet pour 3 essais successifs
- la présence d'une étoile indique une passerelle qui n'a pas répondu. (surcharge du réseau)

Quelque fois, le nom n'apparaît pas (volonté de cacher les adresses ou pas de nom associé)

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, ... et bien sur ... les voitures.

En plus la position des objets mobiles sera connue en permanence grâce au GPS ("Global Positioning System") ou au nouveau projet européen en cours de développement.

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.

Internet aujourd'hui

Actuellement c'est la version 4 ("IPv4") du protocole IP qui est utilisée pour permettre aux machines de dialoguer entre elles. Ce qui ne va pas sans poser de multiples 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 une nouvelle version d'IP est en chantier

Internet de demain

Actuellement, un réseau IPv6 est testé aux Etats-Unis.

Ce réseau s'appelle Internet2. Il a pour but de permettre aux instituts stratégiques (armée, universités, très grosses entreprises) de pouvoir communiquer efficacement maintenant que Internet est saturé par les particuliers qui ne cessent de s'envoyer photos, musiques et films....

Le problème majeur est que IPv6 n'est pas compatible avec IPv4. On prévoit donc un basculement graduel vers IPv6, sans doute en commençant par tous les gros instituts dans le monde.

Les systèmes d'exploitation (Unix, Linux, MacOS X, Windows...) sont déjà en général capables de comprendre IPv6.

Le basculement se fera par la mise à jour des applications (comme le navigateur et le logiciel de messagerie) un peu comme l'arrivée du premier navigateur avait changé notre mode de fonctionnement.

Commandes réseaux

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 » /?**

Ping

Vérifie la connectivité IP d'un ordinateur utilisant le protocoles TCP/IP en envoyant des messages (requête écho) dans le but d'avoir des réponses d'une machine. Ping utilise le protocole ICMP (Internet Control Message Protocol).
Les réponses à la requête écho, s'affichent, avec les temps des parcours circulaires.
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.

Exercices

Lancer cmd.exe sous Windows (interpréteur de commande)

Dans un premier temps:

Vérifier le bon fonctionnement de la carte réseau

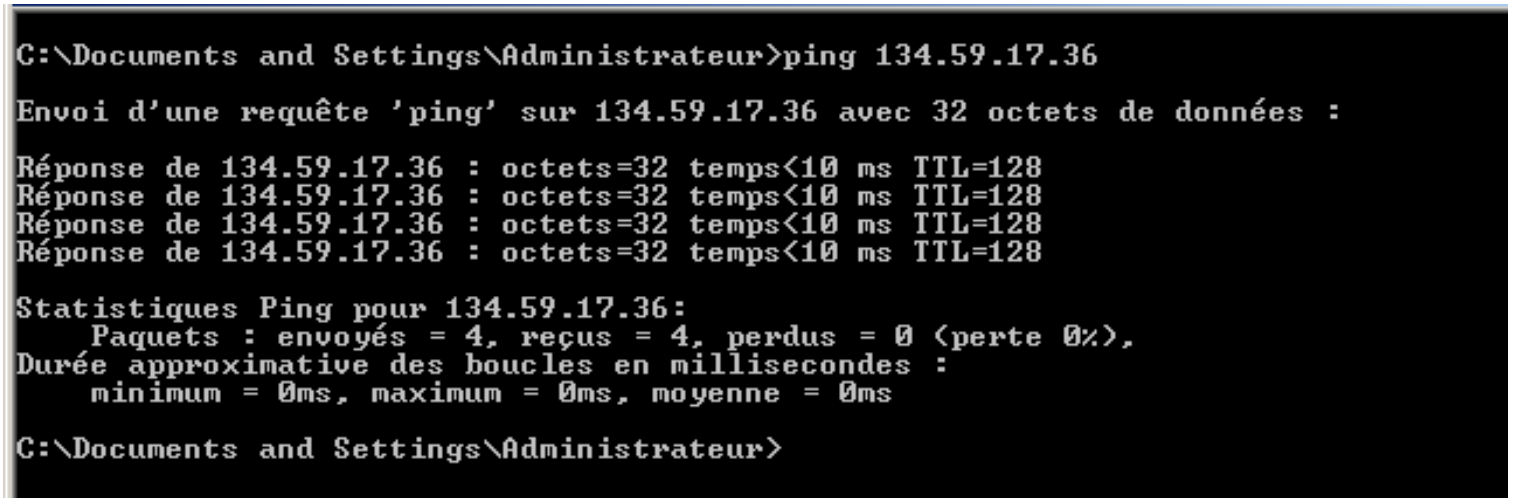
ping 127.0.0.1 (ou localhost)

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

ping 134.59.17.62

Ici il s'agit d'une imprimante !

Serveur Mail de l'université
ping hermes.unice.fr
Adresse IP de cette machine ?



Exercices

Autre exemples:

Pour savoir le nom de la machine => nslookup

nslookup 134.59.17.34

Résultat ?

ping 134,59,17,34

Résultat ?

nslookup 134.157.50.1

Résultat ?

ping 134.157.50.1

Résultat ?

Exercices

Il existe un firewall (pare-feu) qui interdit de faire un ping de la machine.

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 “bioinfo.unice.fr »

tracert hermes.unice.fr

tracert www.kek.jp

tracert www.auckland.ac.nz

Comparez les chemins entre vous.

Commandes réseaux

Nslookup

Affiche des informations que vous pouvez utiliser pour diagnostiquer l'infrastructure DNS (Domain Name System). Affiche les correspondances entre les noms de domaine et les adresses IP.

Tracert (= traceroute sous Unix)

Détermine l'itinéraire vers une destination par la transmission de messages ICMP (messages Requête d'écho).

L'itinéraire affiché correspond à la série d'interfaces de routeurs sur l'itinéraire situé entre un hôte source et une destination. Utilisée sans paramètre, la commande tracert permet d'afficher l'aide.

Commandes réseaux

Ipconfig (=ifconfig sous unix)

Affiche toutes les valeurs de la configuration du réseau TCP/IP et actualise les paramètres DHCP (Dynamic Host Configuration Protocol) et DNS (Domain Name System).

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 (principalement, sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de se trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

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

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.

Note: 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.

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

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)

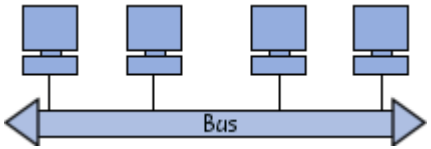
Le support d'interconnexion: c'est le support (généralement filaire, c'est-à-dire sous forme de câble) permettant de relier les ordinateurs entre eux. Les principaux supports utilisés dans les réseaux locaux sont les suivants : supports filaires (le câble coaxial, la paire torsadée, la fibre optique),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

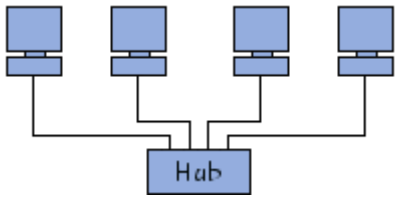
Topologies des réseaux locaux

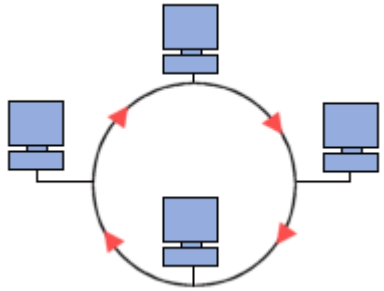
Les dispositifs matériels mis en oeuvre ne sont pas suffisants à l'utilisation du réseau local. En effet, il est nécessaire de définir une méthode d'accès standard entre les ordinateurs, afin que ceux-ci connaissent la manière de laquelle les ordinateurs échangent les informations, notamment dans le 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.

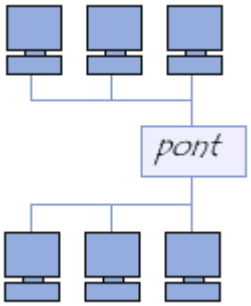
Matériel réseau

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'accés 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), 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
- 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 un numéro que vous composez grâce à votre modem, et qui permet d'établir une connexion.

Les fournisseurs d'accés 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
- une initialisation de la communication
- la vérification du nom d'utilisateur (login ou userid)
- la vérification du mot de passe (password)

Les fournisseurs d'accés 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.

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'accés 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. Quels sont donc ces critères :

• La couverture: certains FAI ne proposent une couverture que des grandes villes (ADSL, cable) , d'autres proposent une couverture nationale.
• 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 (la bande passante allouée à chaque abonné doit être supérieure à sa capacité de transmission afin de lui fournir un service de qualité).
• Le prix: celui-ci dépend du FAI et du type de formule choisie (triplay, etc.).
- illimité en général si ADSL / Cable
- si tél portable / clée 3G :
 * accès gratuit mais avec la communication payante
 * formule dans laquelle le temps de connexion vous est compté, c'est-à-dire que vous ne pouvez pas dépasser un nombre d'heures de connexion par mois, auquel cas les communications subissent une majoration tarifaire
 * un système de forfait mensuel où le temps de connexion est illimité

Les fournisseurs d'accés 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 (parfois 1.35€ l'appel puis 0.34€/min)
- 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.presence-pc.com a fait un très bon comparatif des FAI (mise à jour régulières)
- www.lesproviders.com permet également 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.

Architectures réseaux

Il existe 2 modes de fonctionnement des réseaux :

- **"client/serveur"**, dans lequel un ordinateur central fournit des services réseaux aux utilisateurs

  - exemple des serveurs FTP

- **“poste à poste”** ou **"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

  - exemple du partage de fichier sous windows

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

Inconvéniants 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

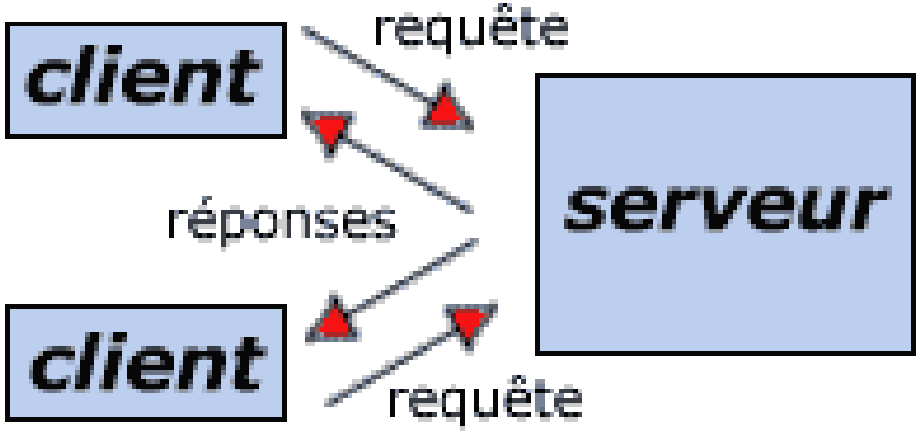
• un maillon faible : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID)

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

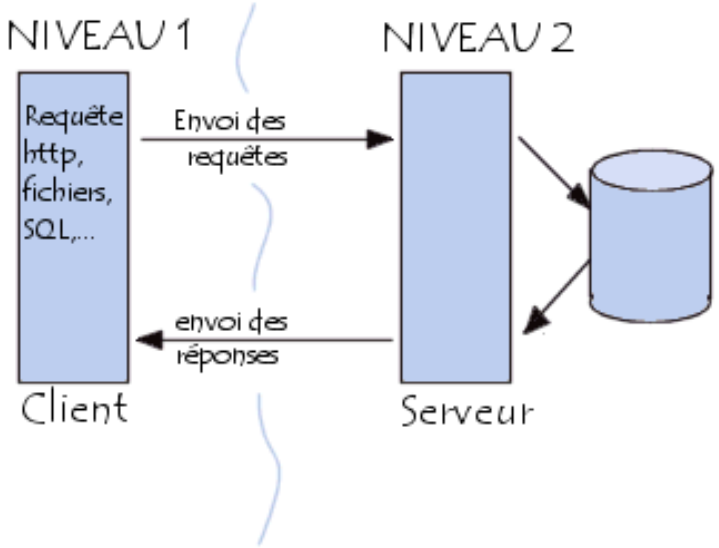
• Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port



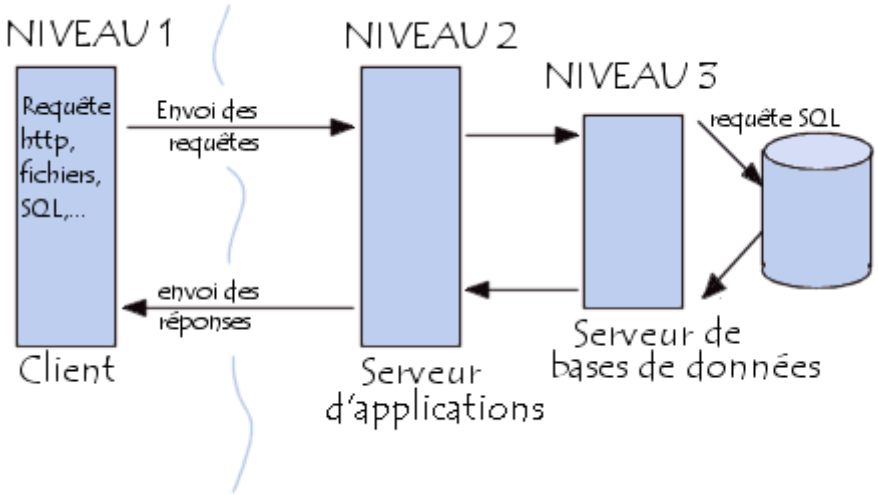
L'architecture client/serveur

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



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.

Le protocole FTP a pour objectifs de :

- permettre un partage de fichiers entre machines distantes
- permettre une indépendance aux systèmes de fichiers des machines clientes et serveur
- permettre de transférer des données de manière efficace

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).

Protocole et serveur FTP

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.

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 »**

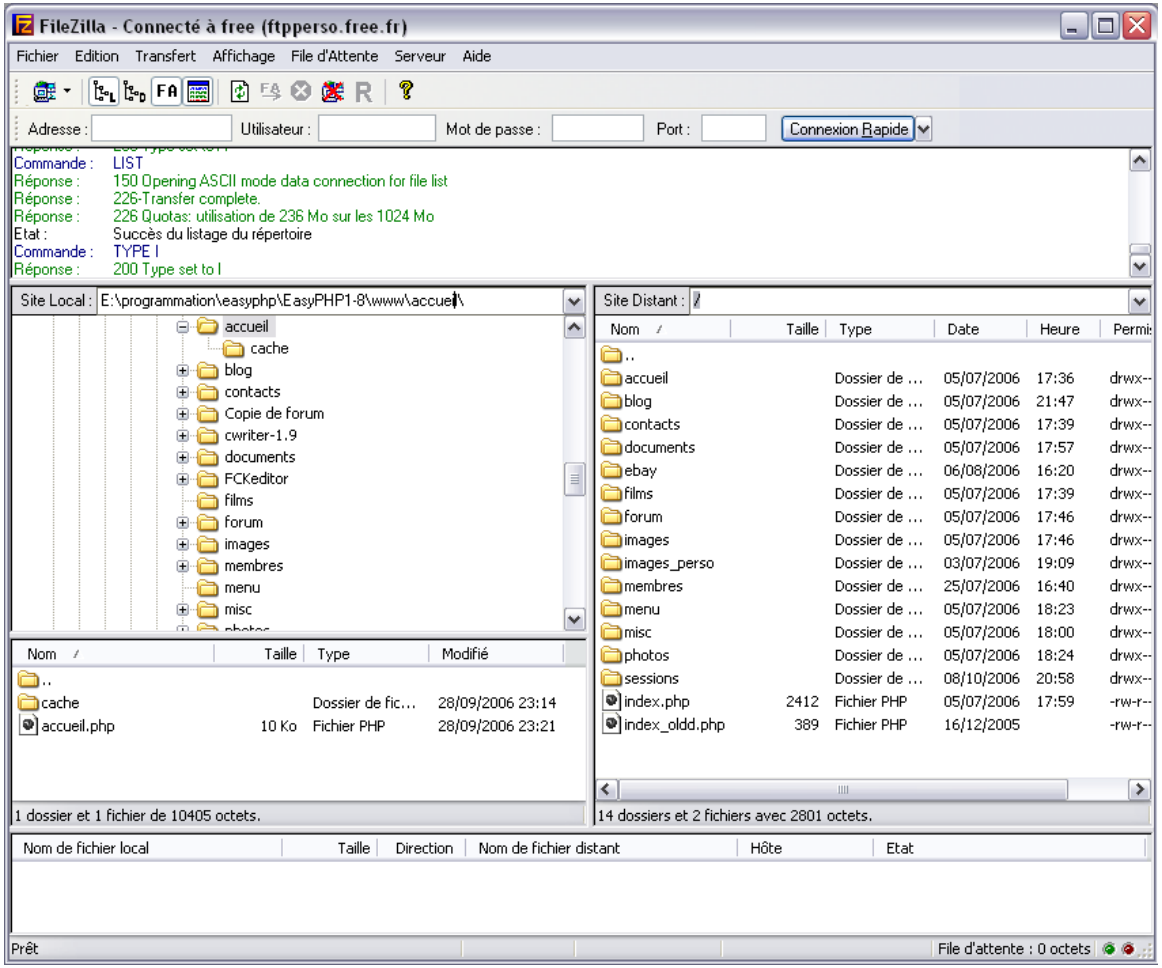
La commande « ftp » (suivie des arguments de connexion) est accessible sur tous les systèmes d'exploitation. Toutes les fonctions sont disponibles mais l'utilisation de ftp en ligne de commande est peu pratique

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



L'architecture client/serveur

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)

L'architecture poste à poste

Présentation de l'architecture d'un système poste à poste

Contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources.

Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés.
Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax etc.)

L'architecture poste à poste

Avantages de l'architecture poste à poste

• un coût réduit (pas de matériel évolué et donc cher, pas de frais d'administration)

• une grande simplicité (la gestion et la mise en place du réseau et des machines sont peu compliquées)

Note: l' « administration » d'un réseau ou de machines désigne :
- Gestion des utilisateurs et de la sécurité
- Mise à disposition des ressources
- Maintenance des applications et des données
- Installation et mise à niveau des logiciels utilisateurs

L'architecture poste à poste

Inconvéniants de l'architecture poste à poste

- Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer ;

- La sécurité est moins facile à assurer, compte tenu des échanges transversaux ;

- Aucun maillon du système ne peut être considéré comme fiable.

Ainsi, les réseaux d'égal à égal sont préférentiellement utilisés pour des applications ne nécessitant pas un haut niveau de sécurité ni une disponibilité maximale (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

L'architecture poste à poste

Fonctionnement d'un système peer to peer

La mise en oeuvre d'une telle architecture réseau repose sur des solutions standards :

- Placer les ordinateurs sur le bureau des utilisateurs
- Chaque utilisateur est son propre administrateur et planifie lui-même sa sécurité

Pour les connexions, on utilise un système de câblage simple et apparent

Il s'agit généralement d'une solution satisfaisante pour des environnements ayant les caractéristiques suivantes :

- Moins de 10-30 utilisateurs
- Tous les utilisateurs sont situés dans une même zone géographique
- La sécurité n'est pas un problème crucial
- Ni l'entreprise ni le réseau ne sont susceptibles d'évoluer de manière significative dans un proche avenir

- Exemple de réseau peer to peer: cette salle informatique
- Cas particulier: les réseaux d'échange de fichiers (avec les logiciels type emule, kazaa, gnutella,...)

L'architecture poste à poste

Exemple d'utilisation du partage de fichiers sous windows

Le partage de fichiers consiste à rendre disponible à travers le réseau le contenu d'un ou plusieurs répertoires. Tous les systèmes Windows possèdent en standard des mécanismes permettant de mettre facilement en partage le contenu d'un répertoire. Néanmoins le partage de fichiers peut poser des problèmes de sécurité, car, par définition, il donne accès aux autres utilisateurs au contenu d'une partie du disque dur.

Lorsqu'un dossier est partagé, les utilisateurs peuvent se connecter à ce dossier par l'intermédiaire du réseau, pour accéder ensuite aux fichiers qu'il contient.

Toutefois, l'accès à ces fichiers n'est possible que s'ils disposent des autorisations adéquates sur les dossiers partagés.

Le partage de fichiers windows ne peut s'appliquer que sur des domaines définis (LAN). Par exemple, il peut s'appliquer entre ordinateurs de cette salle mais ne sera pas utilisable de l'extérieur.

L'architecture poste à poste

Exemple d'utilisation du partage de fichiers sous windows

Autorisations sur les dossiers partagés:

Lorsqu'un dossier est partagé, tous les sous-dossiers et fichiers contenus dans ce répertoire le sont aussi. Les autorisations s'appliquent uniquement aux utilisateurs qui tentent d'accéder à un dossier par l'intermédiaire du réseau.

Pour contrôler l'accès des utilisateurs à un dossier partagé, vous pouvez attribuer des autorisations sur les dossiers partagés

Dans l'Explorateur Windows, un dossier partagé est représenté par une icône en forme de main tenant le dossier partagé.

Note: il est possible d'accéder aux partages de fichiers Windows depuis Linux. Pour cela il faut utiliser le protocole « samba » (par défaut sur tous les Linux)

L'architecture poste à poste

Exemple d'utilisation du partage de fichiers sous windows

Les autorisations sur les dossiers partagés permettent à l'utilisateur

• Lecture

D'afficher les noms de dossiers, les noms de fichiers, les données contenues dans ces derniers et les attributs, d'exécuter des fichiers de programme et de modifier des dossiers dans le dossier partagé.

• Modifier

De créer des dossiers, d'ajouter des fichiers aux dossiers, de modifier des données dans les fichiers, d'ajouter des données aux fichiers, de modifier les attributs de fichiers, de supprimer des dossiers et des fichiers, ou encore d'effectuer les opérations permises par l'autorisation Lecture.

• Contrôle total

De modifier les autorisations au niveau fichier, de s'approprier des fichiers et d'effectuer toutes les opérations permises par l'autorisation Modifier.

Les autorisations peuvent etre gérées par « groupe », un groupe étant un ensemble d'utilisateurs ayant les mêmes droits.

L'architecture poste à poste

Exemple d'utilisation du partage de fichiers sous windows

• **Partage de fichiers simple**

Permet de partager globalement, pour tout le groupe de travail, les fichiers d'un répertoire, sans aucune restriction ni aucun mot de passe.

• **Partages administratifs et partages cachés**

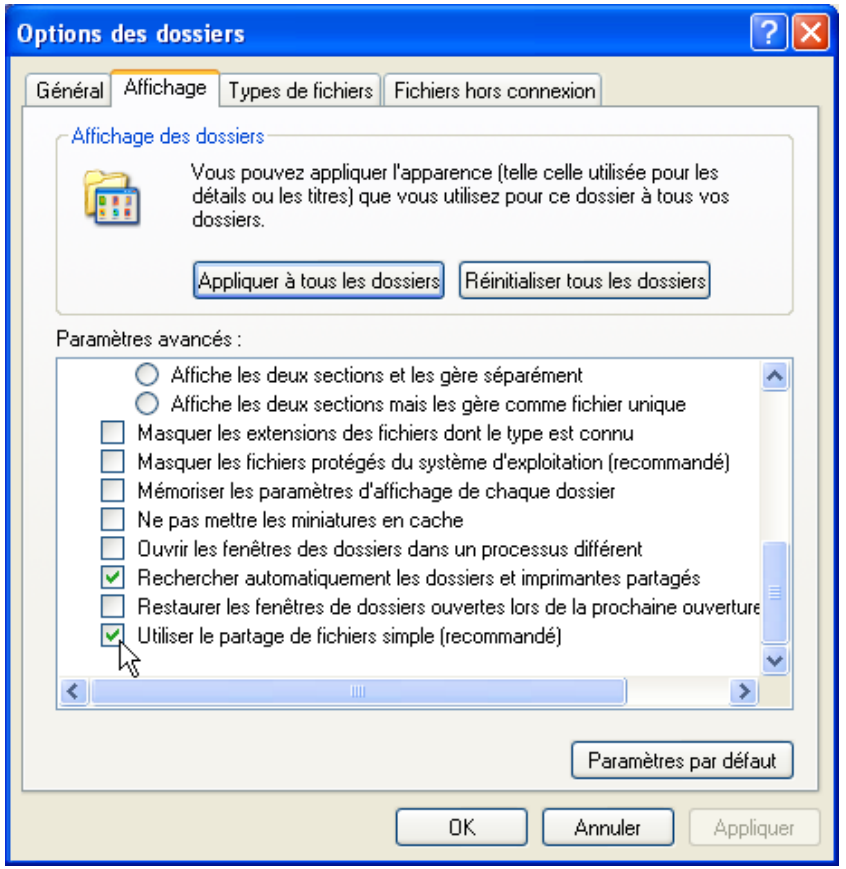
Les partages administratifs par défaut, accessibles uniquement aux administrateurs, sont les suivants :
C$: Accès à la partition ou au volume racine. Les autres partitions sont également accessibles par leur lettre, suivie du caractère « $ » ;
ADMIN$: Accès au répertoire %systemroot%, permettant la gestion d'une machine sur le réseau.
IPC$: Permettant la communication entre les processus réseau.
PRINT$: Accès à distance aux imprimantes.

• **Partage de fichiers avancé** (non dispo sur WinXP home)

Permet de définir des autorisations d'accès aux ressources partagées par utilisateur ou par groupe d'utilisateurs. Contrairement au partage de fichiers simple, l'accès aux ressources partagées se fait suite à l'identification des utilisateurs.

L'architecture poste à poste

Exemple d'utilisation du partage de fichiers sous windows



Exemple d'un partage simple:

- Verifier que le partage simple est activé: poste de travail -> Outils / Options des dossiers... / Affichage. En bas de la liste déroulante, veillez à ce que l'option Utiliser le partage de fichiers simple (recommandé) soit coché.
- Créer un répertoire sur votre disque dur (« tmp » par exemple dans D:\Usagers\partage). Ensuite cliquer avec le bouton droit sur ce répertoire à partager, puis de se positionner sur l'onglet « Partage » et activer le partage (déjà activé sur vos machines et non modifiable....)

- copier un ou plusieurs fichiers dans ce répertoire et vérifier ensuite qu'ils sont accessibles sur d'autres machines : \\adresse_ip\repertoire_partage\ (ou \\nom_machine\\repertoire_partage)

Dans notre exemple: taper dans une fenêtre de l'explorateur: \\ip_voisin\Usagers\tmp\

La même chose est possible par « favoris réseau -> ajouter un favori réseau ». Le partage s'affiche alors dans poste de travail

Copier les fichiers de ses voisins sur vos machines

- Effacer le répertoire partagé.