

‘A toi Chloé Kapapa à la curiosité insatiable’

Remerciement

Je n'ai que 4 personnes à remercier :

- Merci à toi madame mon épouse Chista Katasi pour ta présence et ton accompagnement sans relâche ;
- Merci à toi mon frère Alex Kumwimba pour ton soutient et ta générosité sans précédent ;
- Je dis merci à vous mes chers parents Mukasa wa Kalenga et Ngweji Mujinga pour l'amour que vous ne cessez de manifester à mon endroit.

Avant-propos

L'éducation de base en république démocratique du Congo est l'une des innovations essentielles de la loi cadre n° 14/004 du 11 février 2014 portant organisation et fonctionnement de l'enseignement national.

Cette innovation structurelle du programme national de l'enseignement des sciences qui comprend les sous domaines des mathématiques, des sciences physiques, technologies et technologie de l'information et de communication a engendré un besoin énorme en manuels qui pourront accompagner les apprenants et les enseignants.

C'est pourquoi écrire un ouvrage sur la technologie de l'information et de communication constitue un moyen efficace d'accompagnement au programme d'éducation de base dans son sous domaine **technologie de l'information et de communication.**

Ce manuel est constitué de 9 chapitres qui correspondent aux 9 savoirs essentiels prévus dans le programme national de technologie de l'information et de communication.

Auteur

Table des matières

| | |
|---|----|
| Remerciement..... | 2 |
| Avant-propos | 3 |
| GENERALITE SUR LES RESEAUX INFORMATIQUES | 9 |
| Définition des concepts..... | 9 |
| Rôles d'un réseau..... | 10 |
| Partage de fichiers, partage de ressources et partage de programmes | 10 |
| Partage de fichiers | 10 |
| Partage de ressources..... | 11 |
| Partage de programmes..... | 12 |
| Matériels réseaux | 13 |
| La carte réseau..... | 14 |
| Concentrateur ou le Hub | 14 |
| Le switch (commutateur) et le routeur..... | 15 |
| La topologie réseau | 17 |
| LAN ou réseau local | 17 |
| Les réseaux métropolitains ou MAN | 17 |
| Le réseau étendu ou WAN..... | 17 |
| La topologie physique | 18 |
| La topologie logique..... | 18 |
| LE MODELE TCP/IP ET LE MODELE OSI..... | 22 |
| Différence entre standard et implémentation..... | 22 |
| Un modèle en couche..... | 23 |
| Le modèle OSI | 23 |
| Les rôles des différentes couches sont les suivants..... | 24 |
| Le modèle TCP/IP | 25 |
| Les rôles des différentes couches sont les suivants..... | 25 |
| Encapsulation des données | 25 |
| QUELQUES PROTOCOLES DU MODELE TCP/IP..... | 26 |
| Notions..... | 26 |
| Protocole ARP | 26 |
| Protocole RARP..... | 27 |
| Protocole ICMP | 27 |
| Protocole UDP | 27 |

| | |
|--|----|
| Protocole de Routage | 28 |
| Protocole RIP..... | 28 |
| Protocole OSPF..... | 28 |
| Protocole http..... | 28 |
| Le protocole FTP..... | 29 |
| Protocole Telnet..... | 29 |
| Protocole de Messagerie..... | 29 |
| Le protocole SMTP | 29 |
| Le protocole POP2 et POP3 | 30 |
| Le protocole IMAP..... | 30 |
| Le protocole DHCP..... | 30 |
| RESEAU LOCAL FILAIRE..... | 31 |
| Concepts de base..... | 31 |
| Réseau local filaire | 31 |
| Mode de fonctionnement..... | 31 |
| Architecture égal à égal | 31 |
| Architecture client/serveur | 32 |
| Adresse IP..... | 34 |
| Equipements et rôles..... | 35 |
| Configuration et paramétrage d'un LAN filaire | 36 |
| Matériels nécessaires | 36 |
| Installation d'une carte réseau..... | 37 |
| 1° Installation matérielle (carte réseau)..... | 37 |
| 2° phase : installation des protocoles | 38 |
| 3° Mise en réseau | 38 |
| Paramétrage TCP/IP | 40 |
| RESEAU SANS FIL..... | 41 |
| Concepts de base..... | 41 |
| Modem..... | 41 |
| Carte réseau sans fil | 41 |
| WIFI | 41 |
| Access Point | 41 |
| Catégories et technologies de réseaux sans fil | 41 |
| WPAN (réseau personnel sans fil) | 41 |

| | |
|---|----|
| WLAN ou réseau local sans fil..... | 42 |
| WMAN ou réseau Métropolitain sans fil | 42 |
| WWAN ou réseau étendu sans fil..... | 43 |
| Mode de fonctionnement..... | 43 |
| Avantages et limites | 43 |
| Partage de connexion et configuration | 43 |
| Installation de l'adaptateur sans fil | 43 |
| Configuration du réseau | 43 |
| 1° configuration du point d'accès..... | 44 |
| 2° configuration du réseau sans fil | 45 |
| 3° Configuration des machines clientes..... | 45 |
| Exercice..... | 45 |
| SYSTEMES CLIENT-SERVEUR..... | 47 |
| Sortes des serveurs..... | 47 |
| Serveur des fichiers | 47 |
| Serveur d'impression..... | 47 |
| Serveur de messagerie..... | 47 |
| Serveur web | 47 |
| Serveur de base de données | 48 |
| Serveur d'application..... | 48 |
| Serveur DNS..... | 48 |
| Serveur de licences..... | 48 |
| Serveur Proxy | 48 |
| Les systèmes d'exploitation serveurs..... | 49 |
| Définition..... | 49 |
| Installation d'un serveur et partage de ressources..... | 49 |
| SECURITE INFORMATIQUE | 50 |
| Définition des concepts..... | 50 |
| Sécurité des réseaux..... | 50 |
| Cybercriminalité..... | 50 |
| Cyber attaque..... | 50 |
| Cyber sécurité | 50 |
| Hacking | 50 |
| Cracking | 50 |

| | |
|--|----|
| Sécurité physique | 51 |
| Sécurité logique..... | 51 |
| Malveillance informatique | 51 |
| Virus | 51 |
| Botnet (virus réticulaire)..... | 52 |
| Ver..... | 52 |
| Cheval de Troie | 52 |
| Porte dérobée..... | 52 |
| Bombe logique..... | 52 |
| Logiciel espion..... | 53 |
| Spam ou courrier électronique non sollicité | 53 |
| Attaque sur le web | 53 |
| Injection SQL..... | 53 |
| Cross-site-Scripting | 54 |
| Palimpsestes électroniques..... | 54 |
| Matériel de rebut | 54 |
| Risque liés au réseau sans fil | 54 |
| Luttes contre les malveillances informatiques | 55 |
| Antivirus..... | 55 |
| Mode de fonctionnement des antivirus..... | 55 |
| Quelques antivirus | 55 |
| Pare-feu | 55 |
| Exercice..... | 56 |
| RESEAUX SOCIAUX..... | 57 |
| Concepts de base..... | 57 |
| Réseau social..... | 57 |
| Identité numérique | 58 |
| Sécurité et Confidentialité sur les réseaux sociaux..... | 58 |
| Types de réseaux sociaux..... | 59 |
| Avantages d'utiliser les réseaux sociaux | 60 |
| Problème lié à la sécurité sur les réseaux sociaux | 61 |
| Ethique et morale et observer..... | 61 |
| Exercice..... | 61 |
| INTELLIGENCE ARTIFICIELLE | 62 |

| | |
|---|----|
| Concepts de base..... | 62 |
| Intelligence artificielle | 62 |
| Apprentissage artificiel/automatique ou machine..... | 62 |
| Les différents types d'apprentissage | 62 |
| Big data | 63 |
| Base de données NoSQL | 63 |
| Les différentes catégories des bases de données NoSQL | 64 |
| Domaines d'application de l'intelligence artificielle | 68 |
| Création des ordinogrammes et des algorithmes simples | 69 |
| Algorithme de recherche | 69 |
| Exercice sur le mathématique de 8 ^e éducation base | 73 |

GENERALITE SUR LES RESEAUX INFORMATIQUES

Définition des concepts

Un réseau n'est rien est un groupe d'entité en communication ; il est un ensemble d'objets interconnectés. Il permet de faire circuler des éléments entre chacun de ces objets selon les règles prédéfinis.

C'est quoi une entité ?

Une entité désigne une « chose » parmi d'autres. Par exemple, une personne dans un groupe de personnes est une entité de ce groupe. Pour rester dans cet exemple, on parle de réseau quand deux personnes (entités) parlent ensemble.

Selon le type d'objets, on parlera de :

- **Réseau de transport** : ensemble d'infrastructures et dispositions permettant de transporter des personnes et des biens entre plusieurs zones géographiques ;
- **Réseau téléphonique** : infrastructure permettant de transporter la voix entre plusieurs postes téléphoniques ;
- **Réseau de neurones** : ensemble de cellules interconnectés entre eux ;
- **Réseau de malfaiteurs** : ensemble d'escrocs qui sont en contact les uns avec les autres (un escroc cache généralement un autre) ;
- **Réseau informatique** : ensemble d'ordinateurs reliés entre deux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (des valeurs binaires, c'est-à-dire codées sous forme de signaux pouvant prendre deux valeurs : 0 et 1).

Un réseau informatique n'est rien de plus que deux ordinateurs (ou plus) reliés par un câble (ou dans certains cas par les ondes radio) afin de pouvoir échanger des informations.

Le présent ouvrage s'intéressera bien évidemment aux réseaux informatiques.

Bien entendu il existe d'autres manières d'échanger de l'information entre des ordinateurs sans passer par le réseau (informatique). La plupart d'entre nous a déjà entendu ce que les informaticiens appellent le réseau ***itinérant*** : c'est-à-dire lorsque

vous copiez un fichier sur un CD, un DVD ou une clé USB pour transférer des données sur un autre ordinateur. Le principal problème itinérant est sa lenteur. Un jour des ingénieurs en informatiques ont découvert qu'il était moins coûteux de relier les ordinateurs entre eux par des câbles c'est ainsi que le concept moderne **réseau informatique** est né.

Rôles d'un réseau

Les réseaux informatiques sont destinés à transporter de l'information. Ils peuvent être classés en trois catégories, selon le type et l'origine de cette information (transportée). Le réseau télécom (téléphonique) des opérateurs de télécommunication. Les réseaux informatiques du besoin de communiquer des ordinateurs, et les réseaux de diffusion acheminant les programmes audiovisuels. Chacune de ces catégories présente des caractéristiques particulières, liées aux applications de téléphonie, d'informatique, et de vidéo transportées par les différents réseaux.

Franchement, les réseaux informatiques sont assez pénibles à mettre en place. Alors, pourquoi le faire ? Parce que les avantages que procure un réseau annulent largement la peine que présente son installation. En fait les réseaux sont synonymes de partage. Pour être plus précis, les réseaux permettent de partager trois éléments : les fichiers, les ressources, et les programmes. De manière globale un réseau, un réseau permet l'échange d'informations à distance. On peut donner plein d'application à un réseau : discussion avec une personne, s'échanger des documents, jour en ligne. Le terme application de réseau est l'utilisation (voire exploitation) d'une ressource pour en faire quelque chose de concret. Ici on exploite un réseau pour discuter. En mécanique on peut exploiter du matériel pour faire une voiture.

Partage de fichiers, partage de ressources et partage de programmes

Partage de fichiers

Les réseaux permettent de partager de l'information avec d'autres ordinateurs connectés au réseau. Vous pourrez partager les fichiers de plusieurs manières, en fonction de la configuration de votre réseau. Le moyen le plus direct consiste à envoyer un fichier en pièce jointe à un courrier électronique, depuis votre ordinateur sur

l'ordinateur de votre ami. Ce dernier peut aussi accéder à votre ordinateur par réseau et récupérer le fichier sur votre disque dur. Vous avez également la possibilité de copier le fichier sur le disque dur d'un autre ordinateur puis d'indiquer son emplacement à votre ami pour qu'il puisse le récupérer plus tard. D'une manière ou d'une autre, les données circulent jusqu'à l'ordinateur de votre ami via le câble réseau et non pas via un CD, un DVD ou une clé USB comme dans *le réseau itinérant*.

Partage de ressources

Vous pouvez configurer certaines ressources informatiques comme un lecteur ou une imprimante pour que tous les ordinateurs du réseau puissent y accéder. Par exemple, l'imprimante laser reliée à l'ordinateur P4 dans la **figure 1** est une ressource partagée, ce qui signifie que n'importe qui sur le réseau peut s'en servir. Sans le réseau le poste 1, poste 2 et le poste 3 devraient acheter leurs propres imprimantes laser.

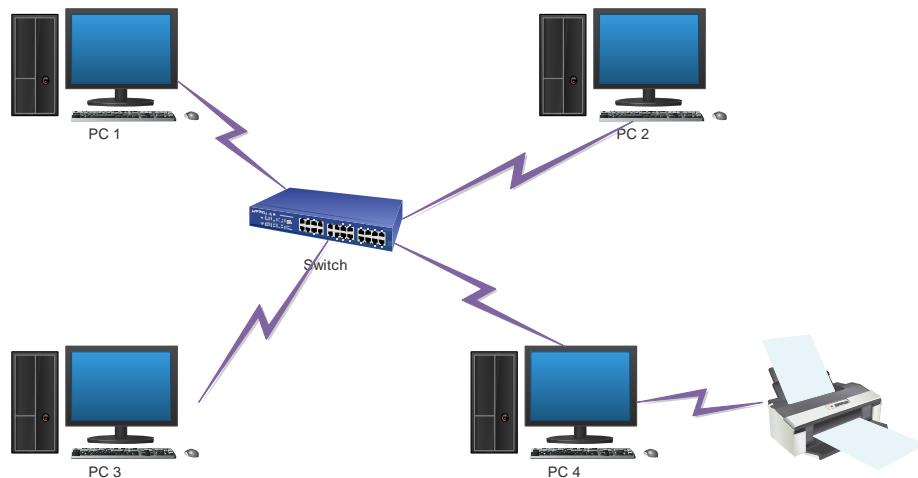


Figure 1 : partage des ressources dans un réseau.

Les lecteurs (partition disque dur) peuvent aussi être des ressources partagées. En fait, vous devez configurer un lecteur en tant que ressource partagée pour pouvoir partager les fichiers avec les autres utilisateurs. Supposez que le poste 1 veuille partager des fichiers avec le poste 2 et qu'un lecteur partagé ait été installé sur le poste 3. Le poste 1 n'a qu'à copier les fichiers sur le lecteur partagé du poste 3 pour indiquer au poste 2 où il l'a stocké. Alors, quand le poste 2 sera disponible, il pourra

copier les fichiers depuis le poste 3 vers le sien (à moins bien sûr que le fournisseur de service de l'ait supprimé).

Vous pouvez partager d'autres ressources, par exemple une connexion internet. En fait, le partage d'une connexion internet est l'une des principales motivations pour la mise en place d'un réseau.

Partage de programmes

Au lieu de conserver des copies distinctes de programmes sur chaque ordinateur, il est parfois conseillé de stocker le logiciel sur un ordinateur partagé auquel chacun peut accéder. Par exemple, dans le cas de dix utilisateur qui choisissent tous le même programme, vous pouvez soit acheter et installer dix exemplaires du programme (un par utilisateur), soit acheter une licence pour dix utilisateurs et installer le logiciel une seule fois, sur le disque partagé. Chacun de ces dix utilisateurs peut alors accéder au programme depuis le disque dur partagé.

Partager des programmes via un réseau consiste à copier le logiciel sur un disque partagé puis à l'installer sur le disque local de chaque utilisateur. Par exemple, Microsoft office vous permet d'opter pour cette solution si vous acheter une licence Microsoft pour chacun des ordinateurs sur lesquels vous installer Office.

L'installation d'office depuis un disque partagé présente un avantage évident : vous n'êtes pas obligé de balader le CD d'installation sur chaque poste. De plus l'administrateur système peut personnaliser l'installation réseau, de sorte que le logiciel s'installe de la même manière sur tous les ordinateurs. Notez toute fois que cette solution est surtout intéressante pour les grands réseaux. Si le vôtre compte moins de dix ordinateurs, il vaut mieux installer office sur chaque machine à partir de CD d'installation.

NB. : rappelez-vous qu'il illégal d'acheter un exemplaire d'un programme pour un seul poste si c'est pour le stocker sur un lecteur partagé afin que tous les utilisateurs du réseau puissent y accéder. Si cinq personnes veulent utiliser, vous devez soit cinq exemplaires du programme, soit une licence réseau qui autorise cinq utilisateurs (ou plus).

Autres avantage du réseau il permet aux utilisateurs de communiquer entre eux, surtout par l'intermédiaire de messagerie électroniques ou de service de messagerie instantanée. Cependant le réseau offre également d'autres moyens de communication : il peut vous servir à organiser des réunions en ligne. Les utilisateurs disposant de caméra vidéo sur leur ordinateur (webcams) peuvent participer à des visioconférences. Vous pouvez même jouer à la « dame de pique » via réseau, pendant votre pause déjeuné, bien évidemment.

Matériels réseaux

Pour créer un réseau vous devez relier tous les ordinateurs de votre bureau ou de votre entreprise avec des câbles et utiliser une carte réseau (carte doté d'un circuit électronique à intégrer dans votre ordinateur et qui dispose d'une prise spéciale à l'arrière de votre ordinateur). Ensuite, vous configurer votre système d'exploitation pour que le réseau fonctionne. Et voilà vous disposez d'un réseau opérationnel.

Si vous ne voulez pas vous encombrer de câbles, vous pouvez opter pour un réseau sans fil. Chaque ordinateur est doté d'un adaptateur spécial équipé d'antennes. Les ordinateurs peuvent ainsi communiquer sans l'aide de câbles.

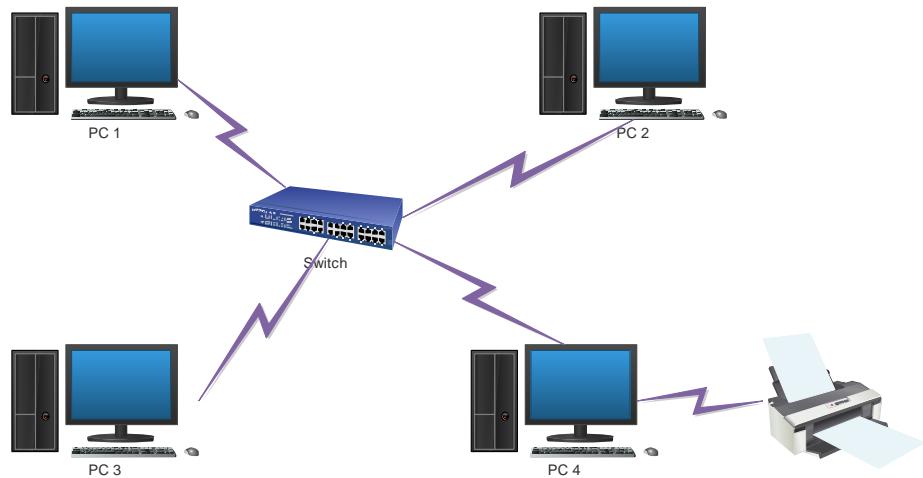


Figure 2 : Matériels réseaux

La figure ci-dessus représente un réseau type, composé de quatre ordinateurs. Vous pourrez voir que les quatre ordinateurs sont connectés via un câble à un appareil nommé switch ou commutateur. Vous pouvez aussi remarquer que l'ordinateur P4 est

connecté à une imprimante. Grâce au réseau, P1, P2, et P3 peuvent utiliser cette imprimante.

La carte réseau

Elle se trouve dans l'ordinateur connecté au réseau ; c'est une carte électronique qui porte le nom carte réseau mais elle est aussi appelée NIC (pour Network interface card). Bien que la NIC soit en général intégrer sur les ordinateurs récents, vous avez la possibilité d'utilise une interface réseau externe reliée à l'ordinateur par le port USB de ce dernier.

La carte réseau est le composant le plus important, elle est indispensable. C'est par elle que transitent toutes les données à envoyer et recevoir du réseau dans un ordinateur. Il n'y a pas grand-chose vous devez connaître, c'est la notion d'adresse MAC : c'est l'adresse physique de la carte. Elle permet d'identifier la machine en réseau, un peu comme une adresse IP. Pour faire court l'adresse physique est relative à la carte réseau ; elle lui est attribué à la fabrication et ne peut pas changer (ce n'est pas tout à fait vrai mais l'idée est là). L'adresse IP est relative au réseau, elle change tout bonnement suivant le réseau.

La carte réseau comporte un port femelle Ethernet : ce port pour accueillir un câble Ethernet mal (connecteur RJ45). Les cartes réseaux internes sont souvent des cartes PCI, c'est-à-dire qu'elles s'enfichent dans un port PCI.

Concentrateur ou le Hub

Un hub est un dispositif réseau qui permet de mettre plusieurs ordinateurs en contact. Définition pas très précise, puisque tout dispositif en réseau (ou presque) a le même but. Bref, ce qu'il faut retenir est qu'un hub est très bête, enfin, moins intelligent que les autres. Ce qu'il fait est tout simple : il reçoit les données par un port, et envoie ce qu'il reçoit aux autres. Il a une interface de réception (un port) et une interface de diffusion (plusieurs autres ports par où les autres ordinateurs sont connectés).

Attention, une interface permet la réception ET la diffusion. Comme vous pouvez le voir sur la photo ci-dessous, le hub n'a pas juste deux interfaces physiques, où on entre par la gauche et on sort par la droite, non !

Le switch (commutateur) et le routeur

Le commutateur ou switch et le routeur sont 2 appareils fondamentalement différents, et pourtant, leurs rôles se ressemblent tellement. Au-delà de leur architecture, il faut comprendre leur différence au niveau d'un réseau.

a. Le commutateur

Le commutateur fonctionne comme le hub sauf qu'il est plus discret et intelligent. Il n'envoie pas ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire. Si l'ordinateur 1 envoie des données à l'ordinateur 2, seul ce dernier les recevra et pas les autres connectés. Afin de déterminer l'ordinateur à qui il faut renvoyer les données le switch se base sur les adresses physiques (adresse MAC) des cartes réseau.

Un commutateur transmet donc des données aux autres ordinateurs en se basant sur leurs adresses MAC. Les transmissions sont plus confidentielles, les autres ne savent rien des données de leur étant pas destinées.

b. Le routeur

Un routeur ressemble à un commutateur sur le plan de l'utilisation : en effet, il permet de mettre plusieurs ordinateurs en réseau. Mais cela va plus loin : **il permet de mettre en contact 2 réseaux fondamentalement différents.**

Dans une petite installation avec un ou plusieurs ordinateurs connectés à une box (qui est en fait un routeur), il est la frontière entre le réseau local et internet. N.B. : notez aussi que le routeur n'est pas uniquement utilisé pour aller sur internet, on l'utilise aussi dans un réseau strictement local.

c. Répéteur

Un répéteur (**repeater** en anglais) agit un peu comme un hub, mais ce dernier n'a que deux interfaces. Son intérêt est de renvoyer ce qu'il reçoit par l'interface de réception sur l'interface d'émission, mais plus fort. On dit qu'il régénère le signal. En transmission sans fil (radio, téléphonie) on parle aussi de relais. Un répéteur permet de couvrir des distances plus grandes que les distances maximales fixées par le matériel que l'on utilise. Par exemple dans un réseau

sans fil(WI-FI) la portée maximale entre 2 appareils est d'environ 50 mètres en intérieur. En plaçant un répéteur peu avant ces 50m, vous pouvez connecter 2 appareils à 100mètres de distance. Le fait que les informations soient renvoyées « plus fort » peut dégrader la qualité du signal dans le réseau sans fil. Pour prendre un exemple, en téléphonie, si l'on se trouve trop loin d'un relais, la qualité du son que l'on entend est dégradée.

d. Le câble réseau

Le câble réseau relie les ordinateurs. Il se branche dans le port de la carte réseau, à l'arrière de l'ordinateur. Il existe plusieurs catégories :

- Le câble à paires torsadés non blindés est appelé UTP (**U**shielded **T**wisted **P**air) ;
- Les câbles coaxiaux : qui ressemblent au câble d'antenne de télévision, est appelé « Câble RG-58 » ;
- Le câble en fibre optique : qui relie à grande vitesse des sites éloignés.

| Matériel | Utilisation |
|-----------------------------|--|
| Carte réseau | La carte réseau est le matériel de base indispensable, qui traite tout au sujet de la communication dans le réseau. |
| Concentrateur (hub) | Il permet de relier plusieurs ordinateurs entre eux mais on lui reproche le manque de confidentialité. |
| Commutateur (switch) | Le commutateur fonctionne comme le hub, sauf qu'il transmet des données en se basant sur leur adresses MAC (adresse physique). Chaque machine reçoit seulement ce qui lui est adressé. |
| Répéteur | Le répéteur reçoit des données par une interface de réception et le renvoi plus fort par l'interface d'émission. On parle aussi de relais en téléphonie et radiophonie. |
| Câble réseau | Le câble relie les ordinateurs. Il se branche dans le port RJ45 (Registered Jack 45) à l'arrière de l'ordinateur. Ils peuvent être de type : UTP, STP, fibre optique, coaxial,... |

La topologie réseau

Les topologies réseaux sont différentes formes que peuvent prendre des réseaux. Avant tout il faut connaître quelques types de réseaux, cela aidera à comprendre pourquoi certaines topologies existent.

LAN ou réseau local

Le LAN est l'acronyme qui signifie Local Area Network (réseau local). Le LAN désigne un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une aire géographique par un réseau, souvent à l'aide d'une technologie (Ethernet ou WIFI). Le LAN est un réseau limité à un espace géographique comme bâtiment. Par exemple, l'ensemble des ordinateurs d'une école forme une LAN.

Note : WLAN, Wireless Local Area Network ou Wireless LAN, est un LAN qui utilise la transmission sans fil (WI-FI...). Le mot Wireless signifie sans fil(wire : fil, less : sans). Par exemple, un hotspot WIFI, c'est-à-dire le point d'accès sans fil WI-FI public comme on en trouve dans les lieux publics tels qu'un hôtel, est un réseau local sans fil (WLAN).

Les réseaux métropolitains ou MAN

Les réseaux métropolitains (MAN : Metropolitan Area Network) interconnectent plusieurs réseaux locaux *géographiquement proches* (maximum quelques dizaines de kilomètres) avec un débit important. Ainsi, un réseau métropolitain permet à deux machines distantes de communiquer comme si elles faisaient partie d'un même réseau local.

Le MAN est formé d'équipements réseaux interconnectés par des liens hauts débits (en générale en fibre optique).

Le réseau étendu ou WAN

Un réseau étendu (WAN, Wide Area Network) interconnecte plusieurs réseaux locaux *à travers de grandes distances géographiques*. Le WAN fonctionne grâce à des équipements réseaux appelés routeurs, qui permettent de déterminer le trajet le plus approprié pour atteindre une machine du réseau. Un WAN est en fait une association de plusieurs LAN.

Note : il existe d'autres type de réseaux, tels que PAN (Personal Area Network) réseaux personnels ; TAN (Tiny Area Network) identiques aux LAN mais moins étendues (deux

ou trois machines) ou CAN (Campus Area Network) identiques au MAN avec une bande passante maximale entre tous les LAN du réseau.

Maintenant vous savez les différents types de réseaux, il est temps de parler de la topologie.

Comme nous l'avons dit précédemment, la topologie est l'arrangement physique ou la configuration spatiale du réseau.

Il existe deux types de topologie : **la topologie physique et la topologie logique**.

La topologie physique

La topologie physique est e fait la structure ou l'arrangement physique d'un réseau. C'est donc la forme, l'apparence du réseau. Il existe plusieurs topologie physiques : bus, l'étoile (la plus utilisée), le mesh(topologie maillée), l'anneau, hybride, etc.

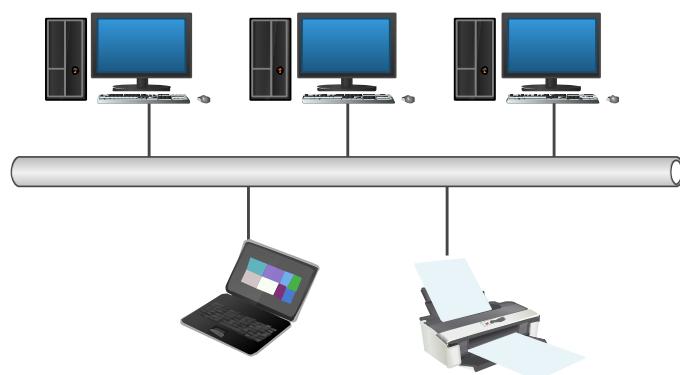
La topologie logique

La topologie logique est la structure logique d'une topologie physique ; elle représente la façon dont les données transitent dans les lignes de communication. Cette topologie définit comment se passe la communication dans la topologie physique. Les topologies logiques les plus courants sont : Ethernet, le Token ring et le FDDI.

1. Réseau en bus (topologie en bus)

Une topologie en bus est l'organisation la plus simple d'un réseau. Dans cette topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire d'un câble, généralement de type coaxial. Dans cette topologie les ordinateurs sont connectés entre eux par le biais d'un seul câble réseau débuté et terminé par des terminateurs. Les terminateurs ont pour but de maintenir les frames

Figure 3 : Topologie en bus

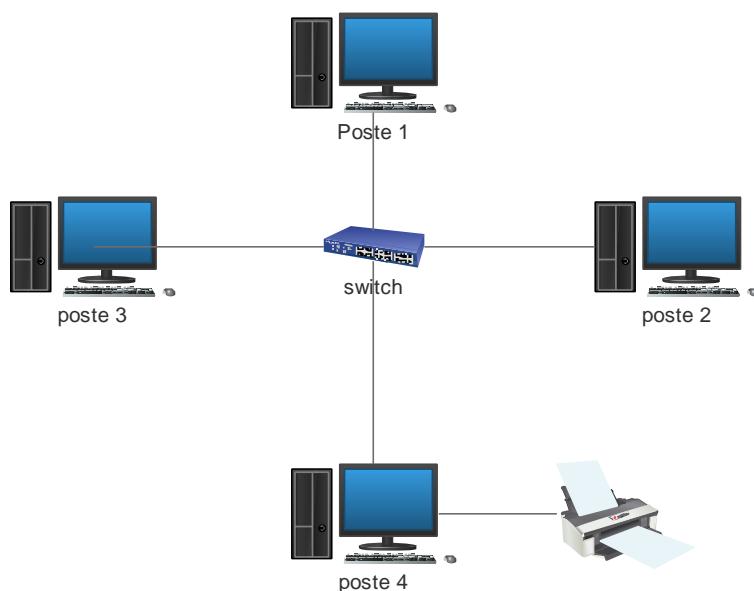


(signaux électrique de données) dans le câble et d'empêcher les « rebonds » des données le long du fil.

Cette topologie est déconseillée pour deux raisons. Le premier est si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté. La deuxième étant donné que le câble de transmission est commun il ne faut pas que 2 machines communiquent simultanément, sinon cela créera des collisions. Pour éviter ce problème, on utilise une méthode d'accès appelée CSMACD, avec cette méthode, une machine qui veut communiquer écoute le réseau pour déterminer si une autre machine est en train d'émettre. Si c'est le cas, elle attend que cette émission soit terminée pour commencer sa communication. Sions, elle peut communiquer tout de suite.

2. La topologie en étoile

Dans la topologie en étoile, les ordinateurs sont connectés (reliés) à une système matériel central (routeur, commutateur, concentrateur, ...). En pratique, dans un réseau d'entreprise en étoile, au centre on trouve un switch. Le principal défaut de cette topologie, c'est si l'élément central ne fonctionne plus, plus rien ne fonctionne : toute communication est impossible. Cependant, il n'y a pas de risque de collision de données.



En revanche un réseau à topologie en étoile est plus onéreux d'un réseau à topologie en bus car un matériel supplémentaire est nécessaire.

3. La topologie en anneau

Dans un réseau possédant une topologie en anneau, les ordinateurs sont théoriquement situés sur une boucle et communiquent chacun à leur tour. C'est un peu comme un réseau en bus avec les ordinateurs disposés en cercle. Ils sont en réalité reliés à un répartiteur (MAU, Multistation Access Unit) qui va gérer la communication entre eux en impartissant à chacun **un temps de parole**. Les deux principales logiques topologiques utilisant cette topologie physique sont Token Ring (anneau à jeton) et FDDI.

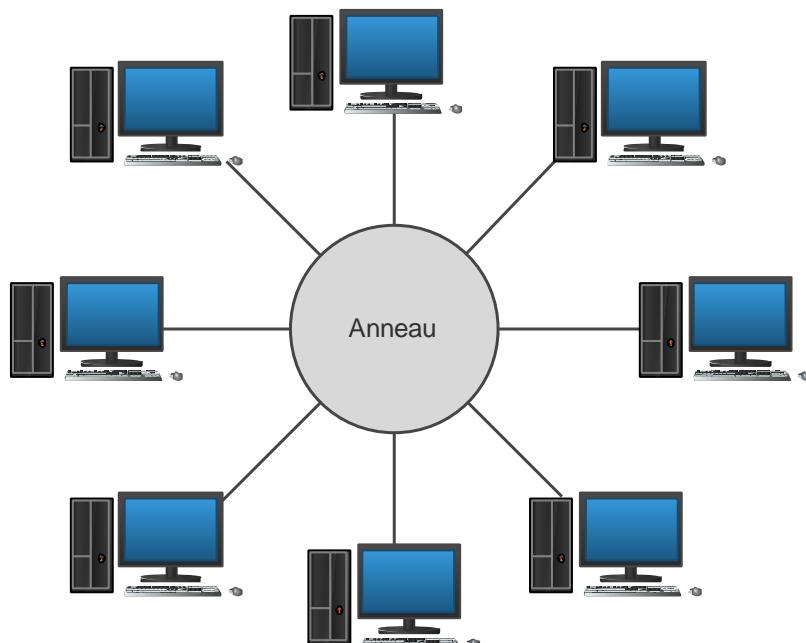


Figure 4 : topologie en étoile.

4. La topologie maillée

Dans la topologie maillée les ordinateurs sont connectés entre eux au moyen des câbles. Comme ça, aucun risque de panne générale si une machine tombe en rade, l'inconvénient de cette topologie ce qu'elle demande beaucoup de câbles. La formule pour connaître le *nombre de cables* est $n \cdot (n - 1)/2$ avec n le nombre d'ordinateur. Donc qu'avec 16 ordinateurs par exemple, ça donnera $16 \cdot (16 - 1)$, soit 120 câbles. En plus chaque câble doit être relié à 2 cartes réseaux, ça ferait $(16-1) \cdot 2$, soit 15 cartes réseaux par machine, soit 240 cartes réseaux en tout. C'est utilisé dans des petits réseaux dans de cas bien précis.

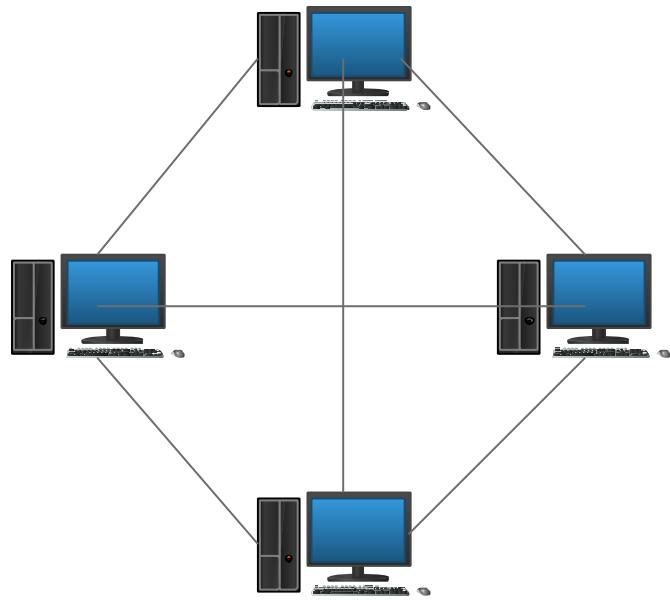


Figure 5 : Topologie maillée.

LE MODELE TCP/IP ET LE MODELE OSI

TCP/IP (Transmission Control Protocol/ Internet Protocol) est une suite de protocoles. Cette appellation provient des noms des deux protocoles majeurs de la suite, c'est-à-dire TCP et IP.

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se fonde sur la notion d'adresse IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. La suite protocolaire TCP/IP est conçue pour répondre à un certain nombre de critère parmi lesquels :

- **Fractionnement des données en paquet** (gestion du format des données) : d'un en-tête et du contenu. L'en-tête correspond aux informations techniques ;
- **Utilisation d'un système d'adresse** (gestion du format d'adresses et correspondances d'adresse) ;
- **L'acheminement des données sur le réseau** (routage) : diriger les données entre deux réseaux ;
- **Détection des erreurs et contrôle de transmission des données** (CRC : cyclic Redundancy Check, contrôle de redondance cyclique) ;
- **Accusé de réception** : certains protocoles permettent à un hôte récepteur d'informer un hôte émetteur qu'il a reçu le paquet envoyé pour empêcher ce dernier de renvoyer les mêmes choses. D'autres par contre n'implémentent cette fonction ;
- **La direction et gestion du flux** d'informations : A et B peuvent-ils communiquer (s'échanger des données) simultanément ? Si oui, il s'agit d'un système de communication **full-duplex**. Sinon il s'agit d'un système de communication **half-duplex**. Un protocole doit donc dicter la direction de flux dans la communication pour empêcher à deux hôtes de communiquer simultanément dans un système half-duplex par exemple.
- **Contrôle de séquences** : toute information envoyée sur un réseau est segmentée en plusieurs « séquences », elles sont ensuite envoyées au destinataire.

Différence entre standard et implémentation

TCP/IP regroupe globalement (2) deux notions :

- La notion de standard : TCP/IP représente la façon dont la communication s'effectue sur un réseau ;
- La notion d'implémentation : l'appellation TCP/IP est souvent étendue aux logiciels basés sur le protocole TCP/IP. Elle est en fait un modèle sur lequel les développeurs d'applications réseau s'appuient. Les applications sont ainsi des implémentations du protocole TCP/IP.

Un modèle en couche

Afin de pouvoir appliquer TCP/IP à n'importe quelle machine, c'est-à-dire indépendamment du système d'exploitation, le système de protocoles TCP/IP a été décomposé en plusieurs modules effectuant chacun une tâche précise. Ces tâches sont réalisées les unes après les autres dans un ordre précis ; on obtient donc un système stratifié que l'on appelle **modèle en couche**.

Le terme de couche est utilisé pour évoquer le fait que les données qui transitent sur le réseau traversent plusieurs protocoles. Ainsi, les données (paquet d'informations) qui circulent sur le réseau sont traitées successivement par chaque couche, qui vient rajouter un élément d'information (en-tête) puis sont mises à la couche suivante.

L'intérêt d'un modèle en couche est de séparer en différentes parties (les couches) selon le niveau d'abstraction. Ainsi, chaque couche du modèle communique avec une couche adjacente, utilise les services de la couche inférieure et fournit des services à la couche supérieure.

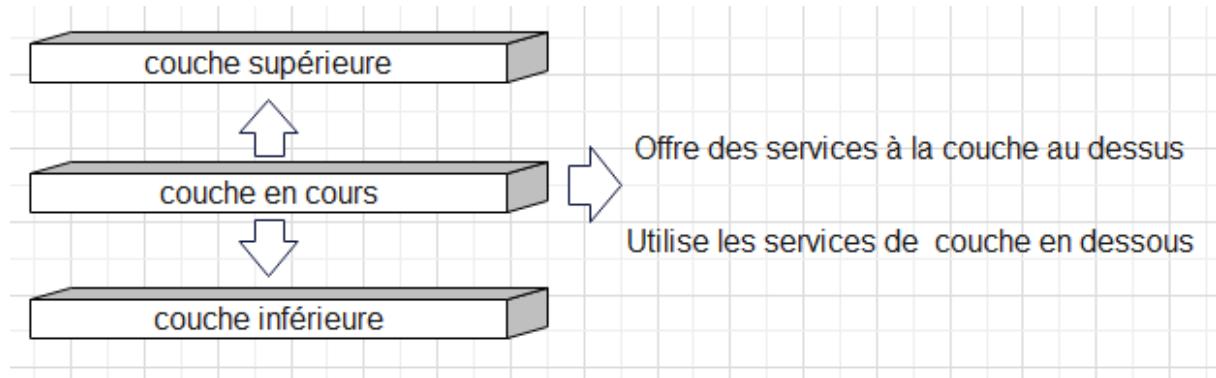


Figure 6 : Fonctionnement des modèles en couche.

Le modèle OSI

Le modèle OSI (Open System Interconnection ou interconnexion de système ouverts) a été mis en place en 1978 par l'ISO (International Standard Organisation, organisation internationale de normalisation, organisation internationale des Standardisation, www.iso.org) afin de normaliser les communications entre les ordinateurs d'un réseau. Ce modèle fut créé à vocation normative, c'est-à-dire pour servir de référence dans le déroulement de la communication entre deux hôtes. D'ailleurs, il est également connu sous le nom OSI reference model (modèle de référence OSI), ou OSI-RM.

En effet aux origines, des réseaux, chaque constructeur avait un système propre (système propriétaire) et nombreux incompatibles coexistaient. Ce modèle a permis de standardiser la communication entre les machines que différents constructeurs puissent mettre au point des produits (matériels ou logiciels) compatibles (pour peu qu'ils respectent scrupuleusement le modèle OSI).

Le modèle OSI est un modèle qui comporte 7 couches distinctes, dans chaque couche opèrent un ensemble de protocole ; tandis que le modèle TCP/IP n'en comporte que 4. En réalité le modèle OSI a été développé un peu plus tard que le modèle TCP/IP, c'est la raison pour laquelle il s'en inspire mais n'est pas tout à fait conforme à ses spécifications.

| Niveau | Couche |
|----------|---------------------------|
| Niveau 7 | Couche application |
| Niveau 6 | Couche présentation |
| Niveau 5 | Couche session |
| Niveau 4 | Couche transport |
| Niveau 3 | Couche réseau |
| Niveau 2 | Couche liaison de données |
| Niveau 1 | Couche physique |

Les rôles des différentes couches sont les suivants

- **Couche Application** : assure l'interface avec les applications. Il s'agit du niveau le plus proche des utilisateurs, gérés directement par les logiciels. Plusieurs protocoles opèrent dans cette couche, dont FTP (pour le transfert des fichiers), Telnet (pour l'établissement des sessions à distances), SMTP (pour l'envoi d'u mail) ;
- **Couche présentation** : définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et chiffrement) indépendamment du système d'exploitation. Par exemple un fichier codé en **EBCDIC** (extended Binary Coded Decimal Interchange Code) vers un fichier codé en ASCII (American Standard Code for Information Interchange) ;
- **La couche session** : définit l'ouverture et la fermeture des sessions de communication entre les machines du réseau ;
- **La couche Transport** : elle est chargée du transport des données, leur découpage en paquets ou segments (séquences) et la gestion d'éventuelles erreurs de transmission. Le protocole TCP/IP est le plus utilisé dans cette couche ;
- **Couche Réseau** : permet de gérer l'adressage et le routage ou relai des données du point A vers le point B, c'est-à-dire leur acheminement vers le réseau. Le protocole le plus utilisé à ce niveau est le protocole IP ;
- **Couche liaison de données** : définit l'interface avec la carte réseau et partage du média de transmission. Là où la couche réseau crée une liaison logique, elle, crée une liaison physique entre les deux hôtes. Les protocoles les plus utilisés dans cette couche : Ethernet, PPP (Point to point Protocol), HDLC (High-level Data Link), etc.
- **La couche physique** : définit la façon dont les données sont physiquement converties en signaux numériques sur les médias de communication (impulsions électriques, modulation de la lumière, etc.). Dans cette couche on y trouve des services tels que la détection des collisions, le multiplexing, la modulation, le circuit switching, etc.

Le modèle TCP/IP

Le modèle TCP/IP fut créé dans les années 1970 par le département de la défense des Etats unis d'Amérique, plus précisément par l'agence DARPA (Defense Advanced Research Project Agency). C'est pour cette raison que vous trouverez aussi sous l'appellation DoD Model pour Department of Defense Model (modèle du département de la défense). Le modèle est créé pour une vocation descriptive, c'est-à-dire il décrit la manière hiérarchisée les règles nécessaires au bon déroulement de communication dans un réseau. Ces règles sont nombreuses et sont classées en catégorie appelées couches.

Le modèle TCP/IP reprend l'approche modulaire du modèle OSI (utilisation des modules ou couches) mais ne contient, lui, que quatre couches. Ces couches ont des tâches beaucoup plus diverses étant donnée qu'elles correspondent à plusieurs couches du modèle OSI.

| Niveau | Modèle TCP/IP | Modèle OSI | Protocoles |
|----------|---------------------|---------------------------|--|
| Niveau 4 | Couche Application | Couche application | Application réseau (Telnet, SMTP, FTP) |
| | | Couche présentation | |
| | | Couche session | |
| Niveau 3 | Couche transport | Couche transport | TCP ou UDP |
| Niveau 2 | Couche Internet | Couche réseau | IP, ARP, RARP |
| Niveau 1 | Couche accès réseau | Couche liaison de données | FTS, FDDI, Ethernet, Token ring |
| | | Couche physique | |

Les rôles des différentes couches sont les suivants

- **Couche d'accès réseau** : spécifie la forme sous laquelle les données doivent être acheminé quel que soit le type de réseau utilisé ;
- **La couche Internet** : est chargé de fournir le paquet de données (datagramme) ;
- **La couche Transport** : assure l'acheminement des données ainsi que le mécanisme permettant de connaître l'état de la transmission ;
- **La couche Application** : englobe les applications standards du réseau.

Encapsulation des données

La transmission dans le modèle OSI et dans le modèle TCP/IP se fait comme suit : quand un hôte A envoie un message à un hôte B, le processus d'envoi va de la couche application 7 (OSI) ou couche 4 (TCP/IP) à la couche 1 (physique) ou la couche 7 (Accès réseau) pour TCP/IP, quand il s'agit de recevoir, le message emprunte le chemin inverse : il part de la couche physique (modèle OSI) ou accès réseau (modèle TCP/IP) pour arriver à la couche application. A chaque passage d'une couche à l'autre lors de l'envoi du message une information est ajoutée au paquet de données, il s'agit d'un en-tête, un ensemble d'information techniques qui garantit la transmission. Au niveau

de la réception, lors du passage dans chaque couche l'en-tête est supprimé. Ainsi à la réception, le message est dans son état d'origine.

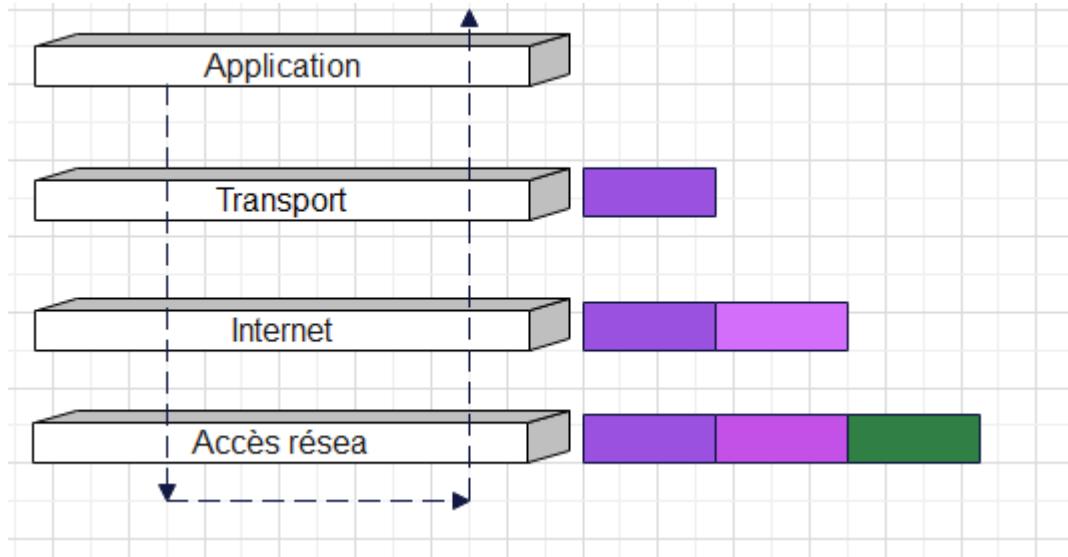


Figure 7 : Modèle TCP/IP : encapsulation des données.

QUELQUES PROTOCOLES DU MODELE TCP/IP

Notions

TCP/IP (Transmission Control Protocol/Internet Protocol) est une suite de protocoles. Cette appellation provient des noms des deux protocoles majeurs de la suite, c'est-à-dire TCP et IP.

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se fonde sur la notion d'adresse IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données.

Protocole ARP

Le protocole ARP a un rôle phare parmi les protocoles de la couche Internet de suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle **protocole de résolution d'adresse (ARP, Adress Resolution Protocol)**. ainsi il permet de faire la correspondance des adresses physiques (MAC ou Média Access Control) aux adresses logiques (Adresse IP).

Le protocole ARP interroge les machines du réseau pour connaître leurs adresses physiques, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans la mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. Les machines du réseau vont comparer cette adresse logique à la leur. Si l'une d'entre elles s'identifie à cette adresse, la

machine va répondre à ARP qui va stocker le couple d'adresse dans la table de correspondance et la communication va alors avoir lieu.

Protocole RARP

Le protocole RARP (Reverse Adress Resolution Protocol) est beaucoup moins utilisé, il signifie protocole ARP inversé, il s'agit donc d'une sorte d'annuaire inversé des adresses logiques et physiques.

En réalité le protocole RARP est essentiellement utilisé pour les stations de travail n'ayant pas de disque dur et souhaitant connaître leur adresse physique.

Le protocole RARP permet à une station de connaître son adresse IP à partir d'une table de correspondance entre adresse MAC (physique) et adresse IP hébergée par une passerelle (Gateway) situé sur le même réseau local (LAN)

Protocole ICMP

Le protocole ICMP (Internet Contrôle Message Protocol), est un protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Étant donné le peu de contrôle que le protocole IP réalise, il permet non pas de corriger des erreurs mais de faire part de ces erreurs aux protocoles des couches voisines ainsi, le protocole ICMP est utilisé par tous les routeurs, qu'ils l'utilisent pour signaler une erreur (appelée Delivery Problem).

Le message d'erreur ICMP sont transportés sur le réseau sous forme de datagramme, comme n'importe quelle donnée. Ainsi les messages d'erreur peuvent eux-mêmes être sujet d'erreurs. Toutefois en cas d'erreur sur un datagramme transportant un message ICMP, aucun message d'erreur n'est délivré pour éviter un effet « Double de neige » en cas d'incident sur le réseau.

Protocole UDP

L'**UDP**, pour User Datagram Protocol, désigne un protocole de communication utilisé sur Internet. On le traduit en français par protocole de datagramme utilisateur.

Défini par la RFC 768 de l'IETF, l'**UDP** permet la transmission de données entre deux entités avec une grande facilité, chacune d'entre elles possédant une adresse IP propre et un numéro de port.

Le protocole UDP (User Datagram Protocol) est un protocole non orienté connexion de la couche Transport du modèle TCP/IP. Ce protocole est très simple étant donné qu'il ne fournit pas de contrôle d'erreurs (il n'est pas orienté connexion)

L'en-tête du segment UDP est simple :

| Port source | Port destination |
|-----------------------|-------------------------------|
| Longueur (16 bits) | Somme de contrôle (16bits) |
| Données | |
| Longueur variable | |

Avec :

- Port source : numéro du port correspondant à l'application émettrice du segment UDP. Ce champ représente une adresse de réponse pour le destinataire ;
- Port destination : contient le port correspondant à l'application de la machine destinataire à laquelle on s'adresse.
- Longueur : ce champs précise la longueur totale du segment, en-tête y compris ;
- Somme de contrôle : il s'agit d'une somme de contrôle réalisé de façon à pouvoir contrôler l'intégrité du segment.

Protocole de Routage

Les routeurs sont des dispositifs permettant de « choisir » le chemin que les datagrammes vont emprunter pour arriver à destination. Il s'agit des machines ayant plusieurs cartes réseaux dont chacune est reliés à un réseau différent. Ainsi, dans la configuration la plus simple, le routeur n'a qu'à « regarder » sur quel réseau se trouve un ordinateur pour lui faire parvenir les datagrammes en provenance de l'expéditeur. Les routeurs fonctionnent grâce aux tables de routage et protocoles de routages.

Protocole RIP

Le protocole RIP (Routing Information Protocol ou protocole d'information de routage) est un protocole de type **vector distance** (vecteur distance), c'est-à-dire que chaque routeur communique aux autres la distance qui le sépare (**nombre de saut qui le sépare**). Ainsi, lorsqu'un routeur reçoit un de ces messages il incrémente cette distance de 1 et communique le message aux routeurs directement accessibles. De cette façon le routeur peuvent stocker l'adresse du routeur suivant dans la table de routage de telle façon que le nombre de sauts pour atteindre un réseau soit minimal. Toutefois ce protocole ne prend en compte que la distance entre deux machines en termes de saut, mais il ne considère pas l'état de liaison afin de choisir la meilleure bande passante possible.

Protocole OSPF

Le protocole OSPF (Open Shortest Path First) est plus performant que le protocole RIP et comme donc à le remplacer petit à petit. Il s'agit d'un protocole de type Protocole Route-Link (que l'on pourrait traduire par **protocole d'état de liens**), cela signifie que, contrairement à RIP, ce protocole n'envoie pas aux routeurs adjacents le nombre de saut qui le sépare mais **l'état de la liaison qui le sépare**. De cette façon, chaque routeur est capable de dresser une carte de l'état du réseau et peut par conséquent choisir à tout moment la route la plus appropriée pour un message donné.

Protocole http

Le protocole http (HyperText Transfer Protocol) est le protocole le plus utilisé sur internet depuis 1990. Le but du protocole http est de permettre un transfert des fichiers localisés (essentiellement au format HTML) grâce à une chaîne de caractères appelée

URL entre un navigateur (le client) et un serveur web (appelé d'ailleurs httpd sur les machines UNIX).

Le protocole FTP

Le protocole FTP (File Transfer Protocol) est, comme son nom l'indique un protocole de transfert des fichiers. Son rôle est de définir la façon selon laquelle des données doivent être transférées sur un réseau TCP/IP. Ce protocole a pour objectif :

- De partager de fichiers entre machines distantes ;
- Permettre une indépendance aux systèmes de fichiers des machines clientes et serveurs ;
- Permettre de transférer des données de manière efficace.

Ce protocole s'inscrit dans un modèle client-serveur c'est-à-dire qu'une machine envoie des ordres (le client) et que l'autre attend des requêtes pour effectuer des actions (le serveur)

Protocole Telnet

Le protocole Telnet est un protocole standard d'internet permettant l'interfaçage de terminaux et d'application à travers internet. Ce protocole fournit les règles de base pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un interpréteur des commandes (coté serveur).

Ce protocole repose sur trois concepts fondamentaux :

- Le paradigme du terminal réseau virtuel (NVT, Network Virtual Terminal) ;
- Le principe d'options négociées ;
- Les règles de négociation.

N.B. : ce protocole est un protocole de base sur lequel s'appuient certains protocoles de la suite TCP/IP (FTP, SMTP, POP3,...).

Protocole de Messagerie

Le courrier électronique est considéré comme 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

Le protocole SMTP (Simple Mail Transfer Protocol, traduit en 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 (PPP).

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 de ces commandes envoyées par le client

(validée par une chaîne de caractères ASCII CR/LF équivalent à un appui sur la touche entrée) est suivie d'une réponse du serveur SMTP composé d'un numéro descriptif.

Le protocole POP2 et POP3

Le protocole POP (Post Office Protocol que l'on peut traduire par protocole de bureau de poste) permet comme son nom l'indique, d'aller récupérer son courrier sur le serveur distant ((le Serveur POP). Il est nécessaire pour les personnes n'étant pas connectées en permanence à internet afin de consulter les mails reçus hors connexion.

Il existe deux principales versions de ce protocole, POP2 et POP3, auxquelles sont affectés respectivement les ports 109 et 110 et fonctionnant à l'aide des commandes textuelles radicalement différentes.

Tout comme dans le cas du protocole SMTP, le protocole POP (POP2 et POP3) fonctionne grâce à des commandes textuelles envoyées au serveur POP. Chacune de ces commandes envoyées par le client (validée par une chaîne de caractères ASCII CR/LF équivalent à un appui sur la touche entrée) est suivie d'une réponse du serveur SMTP composé d'un numéro descriptif.

Le protocole IMAP

Le protocole IMAP (Internet Message Access Protocol) est un protocole alternatif au protocole POP3 mais offrant beaucoup plus de possibilités :

- Il permet de gérer plusieurs accès simultanés ;
- Il permet de gérer plusieurs boîtes aux lettres ;
- Il permet de trier le courrier selon plus de critères.

Le protocole DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol) 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) : Adresse IP, Masque de sous réseau, adresse de la passerelle par défaut, des serveurs de nom DNS et des serveurs de nom NBS connu sous le nom du serveur WINS sur le réseau Windows.

N.B. : en dehors de ces protocoles, il existe d'autres protocoles de la suite TCP/IP appelés **protocole d'accès réseau**, tels que protocole SLIP, le protocole PPP (Point to Point Protocol).

RESEAU LOCAL FILAIRE

Concepts de base

Réseau local filaire

Un réseau local filaire est un LAN utilisant la technologie Ethernet (réseau en câble RJ45). Dans ce type de réseau les machines sont reliés entre eux grâce aux câbles (paire torsadée, coaxiaux, ...).

Mode de fonctionnement

En élargissant le contexte de la définition aux services qu'apporte le réseau local, il y a lieu de distinguer deux modes de fonctionnement :

- Dans un environnement **d'égal à égal** (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 (serveur) fournit des services aux autres (clients).

Architecture égal à égal

Dans une architecture d'égal à égal (ou 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 est un peu serveur et un client. Cela signifie que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder.

Inconvénients

Les réseaux d'égal à égal ont énormément d'inconvénients :

- Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer ;
- La sécurité est peu présente ;
- Aucun maillon du système n'est fiable.

Ainsi, les réseaux poste à poste sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications qui nécessitent pas une sécurité (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

Avantages

L'architecture d'égal à égal à tout de même quelques avantages parmi lesquels :

- Un coût réduit (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance) ;
- Simplicité à toute épreuve.

Mise en place d'un réseau poste à poste

Le réseau poste à poste ne nécessitent pas le même niveau de performance et de sécurité que les logiciels réseaux pour les serveurs dédiés. On peut donc utiliser les différentes versions de Windows car tous ces systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

La mise en œuvre d'une architecture réseau repose sur les solutions suivantes :

- Placer les ordinateurs sur le bureau des utilisateurs ;
- Chaque utilisateur est son propre administrateur et planifie lui-même la politique de sécurité ;
- Pour les connexions, on utilise le système de câblage simple et apparent.

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

- Moins de 10 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.

Administration d'un réseau poste à poste

On désigne par le terme administration :

- Gestion des utilisateurs, de la sécurité ;
- La mise à disposition des ressources ;
- La maintenance des applications et données ;
- L'installation et mise à niveau des logiciels utilisateurs.

Dans un réseau poste à poste type, il n'y a pas d'administrateur, chaque utilisateur administre son propre poste. Tous les utilisateurs peuvent partager leurs ressources comme ils souhaitent (sonnées dans le répertoire partagés, imprimante, etc.)

Sécurité d'un réseau poste à poste

La politique de sécurité minimale consiste à mettre un mot de passe à une ressource. Les utilisateurs d'un réseau poste à poste définissent leur propre sécurité et, comme tous les partages peuvent exister sur tous les ordinateurs, il est difficile de mettre en œuvre un contrôle centralisé. Ceci pose également un problème de sécurité globale du réseau car certains utilisateurs ne sécurisent pas du tout leurs ressources.

Architecture client/serveur

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

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

Dans un environnement client-serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est un atout de ce modèle.

Avantages

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

- Des ressources centralisées : les serveurs sont au centre du réseau, ils peuvent gérer des ressources communes à tous les utilisateurs, par exemple une base de données (serveur de base de données), les fichiers (serveurs FTP), la messagerie (serveur de messagerie), l'impression (serveur d'impression) ;
- Une meilleure sécurité : car le nombre de point d'entrée permettant l'accès au réseau est moins important ;
- Une administration au niveau du serveur : les clients ayant peu d'importance dans ce modèle, ils ont moins besoins 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 modifications majeures.

Inconvénients

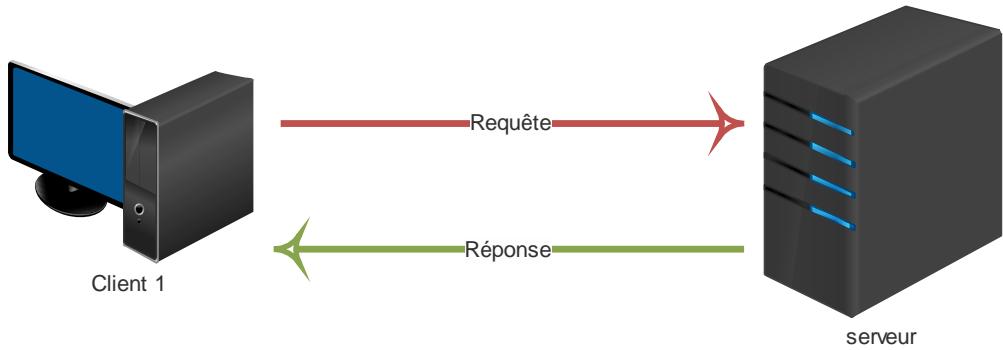
L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- Un coût élevé : dû à la technicité du serveur ;
- Un maillon faible : le serveur est le seul maillon faible du réseau client/serveur. Etant 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 réseau client/serveur fonctionne selon le schéma suivant :

- Le client émet une requête vers le serveur à son adresse et le port qui désigne un service particulier ;
- Le serveur reçoit la demande, et répond à l'adresse de la machine client et son port.



Adresse IP

Sur internet ou dans un réseau local, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresse IP. Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

Adresse IPV4 (Internet Protocol version 4)

Une adresse IPV4 est une adresse 32 bit, comprises entre 0 et 255 comme xxx.xxx.xxx.xxx par exemple 194.153.205.26 est une adresse IPV4. On distingue en fait deux parties dans cette adresse :

- L'ID de réseau (Net-ID) qui désigne le réseau et qui est donné par les nombres de gauche ;
- L'ID d'hôte (host-ID) : qui désigne les ordinateurs de ce réseau et qui est donné par les nombres de droite.

Imaginons un réseau noté 58.0.0.0 les ordinateurs de ce réseau pourront posséder les adresses IP allant de 58.0.0.1 à 58.255.255.24 il s'agit donc d'attribuer les numéros de telle façon qu'il y ait une organisation dans la hiérarchie des ordinateurs et des serveurs.

Ainsi, plus grand est le nombre de bit réservé au réseau, plus petit est le nombre d'ordinateur que va contenir ce réseau vis-versa.

En effet, un réseau noté 102.0.0.0 peut contenir des ordinateurs dont l'adresse peut varier entre 102.0.0.1 et 102.255.255.254 ($256 * 256 * 256 - 2 = 16\,77\,214$ possibilités), tandis qu'un réseau 192.26.0.0 ne pourra contenir que des ordinateurs dont l'adresse IP sera comprise entre 192.26.0.1 et 192.26.255.254 ($256 * 256 - 2 = 65\,34$ possibilités). C'est la **notion de classe d'adresse**.

Les adresses particulières

- Une adresse réseau : est celle dans laquelle la partie host-ID (ou machine) est annulée et est remplacé des zéros. Par exemple pour l'adresse **192.168.12.1** si 1 désigne l'host-ID **192.16.12.0** est une adresse réseau ;
- Adresse machine : lorsque la partie Net-ID est annulée, c'est-à-dire les bits réservés au réseau sont remplacés par des zéros. Cette adresse représente la machine spécifiée par l'host qui se trouve sur le réseau courant. Par exemple

avec l'adresse **129.168.12.1** si **192.168.12.0** désigne le réseau, **0.0.0.1** désigne le client connecté au réseau courant ;

- L'adresse de diffusion (broadcast) : lorsque tous les bits de la partie host-ID sont à 1, permettant d'envoyer un message à toutes les machines situées sur le réseau spécifié par le net-ID. à l'inverse si tous les bits de partie net-ID sont à 1, l'adresse obtenue constitue l'adresse de **diffusion limité** (multicast) ;
- L'adresse lookpack (localhost) : elle désigne la machine locale.

Classes d'adresses

Il y a 3 classes d'adresses. Le but de la division des adresses IP en trois classes A, B, et C'est la facilité de recherche d'un ordinateur sur le réseau.

| Classes | Nombre Possible de réseaux | Nombre d'ordinateurs Possibles maximum |
|---------|----------------------------|--|
| A | 126 | 16 777 214 |
| B | 16 384 | 65 534 |
| C | 2 097 152 | 254 |

Les adresses de classes A sont réservés aux très grands réseaux, tandis l'on attribue les adresses de classe C à des petits réseaux d'entreprise.

Le protocole IPV6 (appelé également IPNG pour IP NEW GENERATION), doit offrir plus de flexibilité et d'efficacité pour résoudre toute variété de problème nouveaux et ne devrait jamais être en rupture d'adresse contrairement au protocole IPV4 permet d'utiliser un peu plus de quatre milliards d'adresses différentes pour connecter les ordinateurs et autres appareils reliés au réseau.

Equipements et rôles

Un réseau local(LAN), est réseau permettant d'interconnecter les ordinateurs d'une organisation ou d'une entreprise ou d'un domicile ; grâce au LAN, il est possible aux utilisateurs d'échanger des informations, de communiquer et d'avoir accès à des divers services.

Un réseau local relie généralement des ordinateurs (ou des ressources telles que des imprimantes) à l'aide des supports de transmission sans fil sur une circonférence d'une centaine de mètres.

Un réseau local est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels, en voici quelques :

- **Carte réseau** : (parfois appelé coupleur) : il s'agit d'une carte électronique connectée à la carte mère et permettant de transmettre l'information ou d'envoyer le signal sans fil ;
- **Tranceiver** (adaptateur) : 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 ;

- **Support physique 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 physiques utilisés dans les réseaux locaux sont les suivants ; le câble coaxial, la paire torsadée, et la fibre optique.
- **Les répéteurs** (repeaters) : permettent de régénérer un signal ;
- Les concentrateurs (hub) : permettent de relier entre eux plusieurs hôtes ;
- **Les ponts** (bridges) : qui permettent de relier des réseaux locaux de mêmes types ;
- Les commutateurs (switches) : qui permettent de relier divers éléments tout en segmentant le réseau ;
- **Les passerelles** (Gateway) qui permettent de relier des réseaux locaux de types différents ;
- **Les routeurs** : permettent de relier de nombreux réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale ;
- **Les B-routeurs** : associent les fonctionnalités d'un routeur et d'un pont ;
- **Le modem** : permet la relation avec internet. De nos jours, les boxes des F.A.I. (fournisseurs d'accès internet) cumulent les fonctions de modem, de routeur, et souvent d'un point d'accès WIFI ;

Certains autres matériels sont spécifiques au **réseau sans fil** :

- **Les points d'accès** : (notés AP pour Access point, parfois appelés bornes sans fil) permettant de donner un accès au réseau filaire (auquel il est raccordé), aux différentes stations avoisinantes équipées de carte WIFI. Dans la plupart des cas, votre AP sera un modem routeur ;
- **Les antennes** : elles sont généralement intégrées, mais certains routeurs et certaines cartes permettent d'adapter une antenne de votre choix à la place de l'antenne par défaut ;
- **Les amplificateurs** : placé entre les équipements et son antenne, pour amplifier le signal.

Configuration et paramétrage d'un LAN filaire

Lorsque vous disposez de plusieurs ordinateurs, il peut être pratique de les connecter ensemble afin de créer un réseau local (LAN). La mise en œuvre d'un tel réseau est très onéreuse et permet entre autre :

- De partager de ressources logicielles (programmes) et matérielles (imprimantes, disque dur partagé, connexion à internet) ;
- La mobilité (dans le cas du réseau sans fil) ;
- La discussion (essentiellement lorsque les ordinateurs sont distants)
- Le jeu en réseau.

Pour créer un réseau local, il suffit d'avoir les matériels suivants :

Matériels nécessaires

1. Matériel général

- Plusieurs ordinateurs ou dispositifs à capacité réseau (ordinateurs fonctionnant sous divers OS peuvent sous certaines conditions appartenir à un même réseau) ;
- Sur chaque machine, une carte réseau Ethernet ou sans fil. Elle peut être sur le port enfiché sur le port PCI, intégré à la carte mère, sur le port USB ou sur le port PCMCIA.

2. Pour le réseau filaire

- Des câbles RJ45, choisissez selon la longueur et selon la catégorie ;
- un concentrateur (Hub), équivalent auquel seront connectés les câbles RJ45 provenant des ordinateurs du réseau, ou mieux un commutateur (switch) pour les meilleures performances.

N.B. : pour connecter deux ordinateurs un seul câble RJ45 croisé suffit.

3. Pour le réseau sans fil

- Un point d'accès (Access point) auquel se connecteront des différents dispositifs. Les boxes des F.A.I. (fournisseurs d'accès internet) sont désormais fréquemment dotés de capacité sans fil et constituant alors un tel un point d'accès.

4. Pour le réseau CPL (courant porteur de ligne)

- pour chaque machine concernée, un adaptateur CPL connecté à une prise de courant et relié au dispositif concerné.

Installation d'une carte réseau

Pour permettre l'échange de données entre les ordinateurs, il est nécessaire d'installer (si elle n'est pas déjà installée) une carte réseau. Son installation se passe en deux phases :

1° Installation matérielle (carte réseau)

Dans cette phase vous devez ouvrir votre ordinateur et d'insérer la carte réseau dans le connecteur d'extension.

Le connecteur d'extension (slots) est un connecteur rectangulaire dans lequel on enfiche les cartes verticalement. Il en existe plusieurs sortes :

- les connecteurs ISA fonctionnant en 16 bits ;
- les connecteurs PCI fonctionnant en 32 bits ;
- les connecteurs PCI Express, version série du PCI parallèle ;
- les connecteurs AGP fonctionnant en 32 bits, il s'agit d'un bus rapide réservé à la carte graphique.

N.B. : une carte réseau (essentiellement sans fil) peut également se connecter sur le port PCMCIA ou USB (on parle souvent de dongle). Il suffit dans ce cas d'insérer la carte ou son connecteur dans le port adéquat sur le boîtier de l'ordinateur.

Si vous avez installé une nouvelle carte réseau, le Système d'exploitation comme Windows détectera le périphérique et le pilote sera installé automatiquement. Si ce

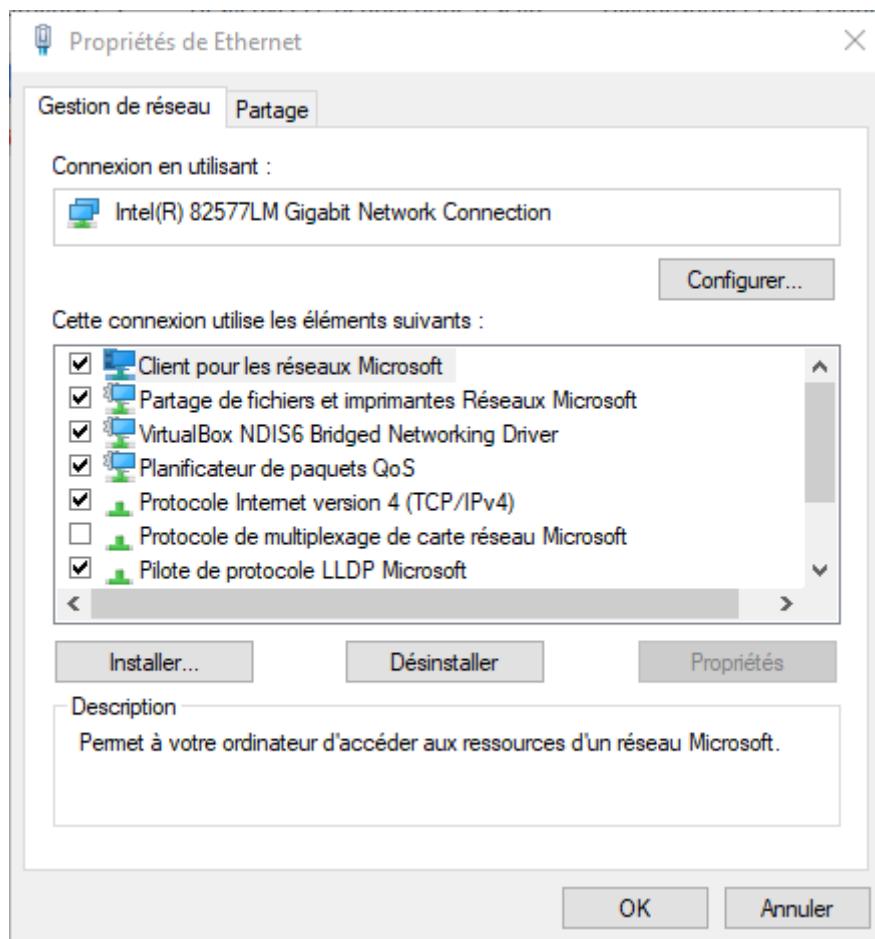
n'est pas le cas visitez le site du constructeur de la carte réseau, télécharger et installer manuellement les pilotes. En cas d'échec visitez la documentation du constructeur dans votre moteur de recherche peut également vous rendre service.

2° phase : installation des protocoles

Les protocoles sont des éléments logiciels qui vont vous permettre la communication entre les ordinateurs. Les principaux protocoles pour un réseau local sont les suivants :

- TCP/IP : le protocole utilisé sur Internet. Il sera nécessaire si vous désirez relier votre réseau local à internet ;
- Client Réseaux Microsoft : le protocole propriétaire de Microsoft, permettant notamment, le partage des fichiers ou d'imprimante.

N.B. : par défaut le S.E. installe le protocole courant, qui seront suffisant pour la quasi-totalité des utilisateurs. Sauf si vous avez des besoins spécifiques dans ce cas, ouvrez les propriétés de la connexion réseau souhaitée et cliquez sur installer, puis choisissez le protocole ou service.



3° Mise en réseau

Une fois vous avez fini l'installation des cartes réseaux dans les ordinateurs, l'installation des pilotes et l'installation des protocoles, il est temps de mettre en réseau les appareils. Cette phase passe en deux étapes :

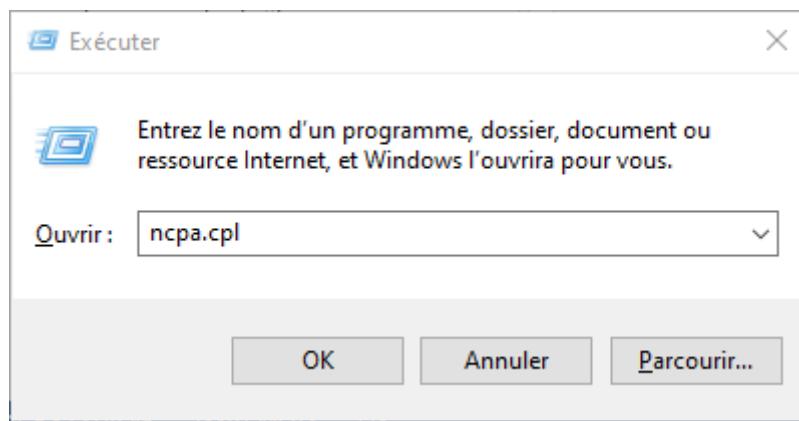
a) Choix de l'architecture du réseau

Dans cette phase vous choisissez la topologie de votre réseau (en étoile pour réseau local en RJ45 recommandé). Dans ce cas les ordinateurs seront chacun connectés au hub (concentrateur) ou switch (commutateur) ou la boîte par l'intermédiaire d'un câble RJ45. La structure d'un réseau ressemble ça.

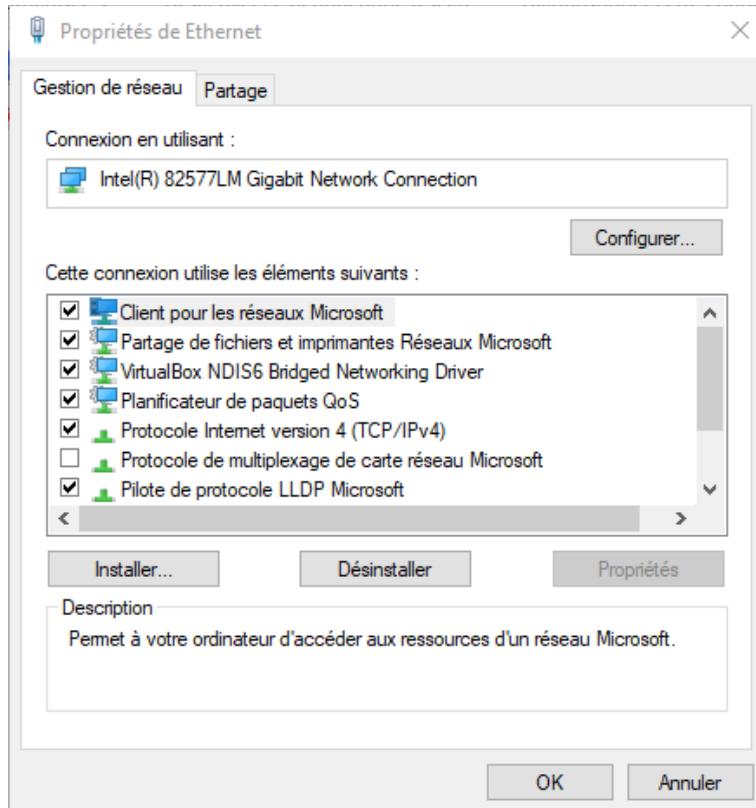
N.B. : si vous désirez connecter deux ordinateurs, passez-vous du hub ou du switch, en reliant directement les deux ordinateurs avec un câble RJ45 croisé.

b) Configuration de la carte réseau

Pour configurer chaque ordinateur (sous Windows), il suffit d'utiliser le raccourci clavier **WINDOWS + R /ncpa.cpl/Ok** comme ceci :



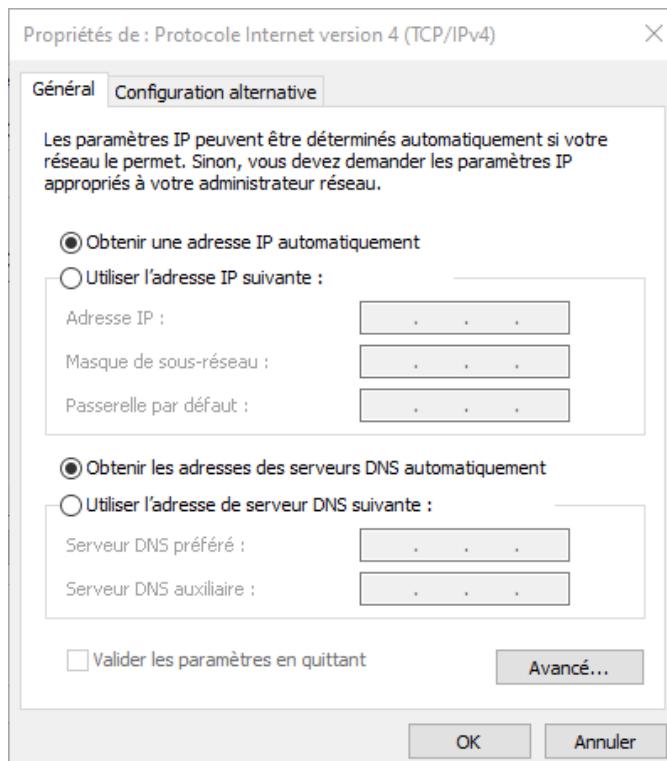
Cliquez-droit sur Réseau local Ethernet/propriétés. Une fois la fenêtre des propriétés Ethernet affiché, vous verrez les différents protocoles installés, il est nécessaire que les protocoles suivants soient installés : clients pour les réseaux Microsoft, protocoles Internet version 4 (TCP/IPV4) et facultativement planificateur des paquets QoS, NetBIOS NwLink, protocole de transport compatible NwLink IPX/SPX (pour les anciens jeux).



N.B. : si l'un de ce protocole venait à manquer, cliquer sur Installer... et ajouter-le.

Paramétrage TCP/IP

Chaque ordinateur doit ensuite se voir affecter une adresse (Adresse IP) afin de pouvoir communiquer, pour cela il s'agit de sélectionner le protocole Internet version 4 (TCP/IPv4) et cliquez sur propriétés.



Si vous disposez d'un routeur, d'une boîte ou d'un serveur DHCP, l'attribution des adresses IP peut se faire automatiquement. Sélectionner [obtenir une adresse IP automatiquement](#).

Si votre point d'accès ne possède pas de serveur DHCP, sélectionnez [utiliser l'adresse IP suivante](#) (en supposant que l'ordinateur 1 est celui qui dispose de l'accès à internet).

| Rubriques | Ordinateur 1 | Ordinateur 2 | ... | Ordinateur x |
|------------------------|---------------|---------------|-----|---------------|
| Adresse IP | 192.168.0.1 | 192.168.0.2 | | 192.168.0.x |
| Passerelle par défaut | 192.168.0.1 | 192.168.0.1 | | 192.168.0.1 |
| Masques de sous-réseau | 255.255.255.0 | 255.255.255.0 | | 255.255.255.0 |

Une fois l'adresse IP allouée, il suffit de fermer la fenêtre en cliquant sur ok (le DNS seront en automatique).

RESEAU SANS FIL

Un réseau sans fil (Wireless network), comme son nom l'indique il s'agit d'un réseau dans lequel deux appareils peuvent échanger les données sans liaison filaire (câblé). Grâce à ce réseau un utilisateur peut rester connecté en déplaçant en même temps, on parle de mobilité (parfois). Ces types de réseaux (sans fil) sont fondés sur une liaison utilisant les ondes radioélectriques (radio et infrarouge) à la place des fils (câbles) habituels.

Il existe plusieurs technologies développées autour du réseau sans fil qui se distinguent **par le débit, la fréquence d'émission et la portée de transmission**.

Concepts de base

Modem

Carte réseau sans fil

WIFI

Access Point

Catégories et technologies de réseaux sans fil

Il existe plusieurs catégories de réseaux sans fil :

WPAN (réseau personnel sans fil)

Le réseau personnel sans fil (appelé également réseau domestique sans fil, et noté WPAN, Wireless personal Area Network) concerne le réseau sans fil d'une faible portée : de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimantes, téléphones portables, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou permettre la liaison sans fil de deux ordinateurs à une très petite distance.

Voici quelques technologies développées autour du réseau personnel sans fil :

- **Le Bluetooth** : est la principale technologie WPAN lancée par la firme Ericsson en 1994, proposant un débit théorique de 1mbps pour une portée maximale d'environ trentaine de mètres. Connue aussi sous le nom IEE 802.15.1, il possède l'avantage d'être peu gourmand en énergie, ce qui le rend particulièrement adapté à une utilisation au sein des petits périphériques.



N.B. : le nom Bluetooth (dent Blue en français) se rapporte au nom du roi danois Herald II (910-986) surnommé **Herald II blatand** (à la dent Blue) à qui on attribue l'unification du suède et de la Norvège ainsi qu'à l'introduction du christianisme dans les pays scandinaves.

- **HomeRF** (Hom Radio Frequency), lancé en 1998 par la firme HomRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et MS) propose un débit de 10 mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. La norme HomeRF soutenue notamment par Intel a été abandonnée en janvier 2003, car les fondeurs de processeurs misent sur désormais sur les technologies WIFI embarquées.



- **ZigBee** : connue sous le nom IEE 802.15.4, permet d'obtenir des liaisons sans fil très bas prix avec une faible consommation d'énergie ce qui la rend très adaptée pour être directement intégrée dans les petits appareils électroniques (appareils électroménagers, HIFI, jouets, ...) cette technologie opère sur la bande de fréquence 2.5 GHZ et sur 16 canaux, permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée théorique de 100 mètres environ. Cette technologie utilise les liaisons infrarouges et largement utilisée dans la domotique (télécommande), toutefois elle souffre des perturbations dues aux interférences lumineuses. L'association (Infrared Data Association) fut formée en 1995 et regroupe plus de 150 membres.

WLAN ou réseau local sans fil

WMAN ou réseau Métropolitain sans fil

Le réseau métropolitain sans fil (WMAN, Wireless Metropiltain Area Network) est un réseau aussi connu sous le nom boucle local Radio (BLR). Ce réseau (Boucle Local

Radio) est basé sur la norme IEEE 802.16. le WMAN un débit de 1 à 10 Mbit/s et une portée de 4 à 10 kilomètres, ce qui destine cette technologie aux opérateurs de télécommunications.

La norme métropolitaine sans fil la plus connue est le WIMAX, permettant d'obtenir des débits de l'ordre de 70 Mbit/s sur un rayon de plusieurs kilomètres. Ce standard intègre notamment la notion de qualité de service (QoS, Quality of Service), c'est-à-dire la capacité à garantir le fonctionnement d'un service à utilisateur.

WWAN ou réseau étendu sans fil

Le réseau étendu sans fil (WWAN, Wireless Wide Area Network) également connu sous le nom de réseau cellulaire mobile. Il s'agit d'un réseau sans fil le plus répandu puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil.

Mode de fonctionnement

Avantages et limites

Partage de connexion et configuration

Un réseau sans fil permet de connecter plusieurs appareils ou plusieurs ordinateurs en réseau, sans aucune connectique filaire possible. Grâce aux technologies réseau sans fil, il est ainsi possible d'accéder à des ressources partagées, notamment à internet, à partir de plusieurs lieux différents : on parle ainsi de mobilité ou d'itinérance.

La technologie WIFI est la technologie de réseau local sans fil la plus usitée. Elle propose deux modes opérationnels :

- **Le mode ad-hoc** : dans ce mode les ordinateurs sont connectés les unes aux autres dans aucun point d'accès afin de constituer un réseau égal à égal ;
- **Le mode infrastructure** : les clients sans fil sont connectés à un point d'accès. Il s'agit généralement du mode par défaut des cartes 802.11b. un mode permettant de connecter à un réseau filaire par l'intermédiaire d'un équipement appelé point d'accès.

Pour mettre en place ce réseau, il faut suivre les étapes suivantes :

Installation de l'adaptateur sans fil

Avant toute chose, il est nécessaire d'équiper toutes les machines du futur réseau d'un adaptateur sans fil et d'installer les nouvelles pilotes. Une nouvelle icône apparaît dans la barre des tâches, indiquant la présence d'un adaptateur dans fil.

Configuration du réseau

La configuration du réseau sans fil dépendra du mode choisi : ad-hoc ou infrastructure.

a) Le mode ad-hoc

Si vous disposez de deux ordinateurs ou plus équipés d'adaptateurs dans fil (carte WIFI), il est possible de les relier très simplement en réseau, en mettant en place un réseau « ad-hoc » c'est-à-dire un réseau égal à égal, sans utiliser le point d'accès.

Si un des ordinateurs du réseau ad-hoc possède une connexion à internet, il est possible de la partager avec les autres ordinateurs du réseau, comme dans le cas d'un réseau filaire traditionnel.

Utiliser la commande suivante pour créer un réseau ad-hoc en donnant le nom du réseau (SSID) et le mot de passe (Key) pour y accéder. Veuillez taper cette commande sous PowerShell en administrateur (Windows+X).

```
netsh wlan set hostednetwork mode = allow ssid=ad-hoc1 key=ad-hoc-key
```

Puis appuyez sur entrée pour valider la commande. Ensuite démarrer le réseau hébergé en tapant la commande suivante :

```
Netsh wlan start hostednetwork
```

Une fois le réseau hébergé démarré, vous n'avez qu'à vous y connecter avec les autres ordinateurs du réseau comme si vous on se connecte sur un point d'accès wifi traditionnel en spécifiant le mode de passe.

N.B. : avant toutes ces manipulations vous devez vérifier si votre adaptateur wifi prend en charge la mise en place d'un réseau hébergé en tapant la commande suivante :

```
Netsh wlan show drivers
```

Si dans le résultat de la commande vous avez : Réseau hébergé pris en charge : oui. Donc vous avez la possibilité de mettre en place un réseau ad-hoc.

Vous pouvez arrêter votre réseau avec la commande

```
Netsh wlan stop hostednetwork
```

b) Le mode infrastructure

La mise en place d'u réseau WIFI en mode infrastructure est très similaire à celle d'un réseau WIFI d'égal à égal à ces quelques différences près :

- Un réseau WIFI en mode infrastructure nécessite un point d'accès, connecté ou non à un réseau local filaire voire à internet dans le cas d'un routeur sans fil ;
- L'association des machines clientes au réseau infrastructure est généralement plus simple ;
- Si le réseau sans fil a pour but de permettre l'accès à internet aux postes nomades, il n'est pas nécessaire de laisser un ordinateur allumé pour obtenir l'accès au réseau des réseaux ;
- Les possibilités en termes de sécurité sont plus larges et plus robustes.

1° configuration du point d'accès

Le point d'accès est l'élément matériel centrale d'un réseau WIFI en mode infrastructure : il permet de gérer l'association des machines clientes et de les relier

au réseau local. Ainsi, un point d'accès possède en générale un certain nombre des connecteurs permettant de le relier à un réseau local ou bien parfois à un ordinateur à l'aide d'un cordon USB.

L'interface de configuration peut varier d'un constructeur à un autre, néanmoins la plupart du temps les points d'accès possèdent un web localisable du type <http://192.168.0.1> (ou <http://192.168.1.1>).

Pour configurer le point d'accès sans fil, il suffit donc que celui-ci soit branché à minima à un ordinateur par une connexion filaire (parfois sans fil). Pour accéder à l'interface, il suffit de saisir l'adresse <http://192.168.1.1> dans un navigateur web. L'interface demande alors un nom utilisateur (identifiant) et mot de passe. Il suffit de saisir l'identifiant et le mot de passe par défaut, mentionnés sans la documentation du point d'accès.

N.B. : il est vivement recommandé de modifier le mot de passe par défaut, afin d'éviter un risque de piratage par un tiers. En effet, l'écran d'invite précise généralement le nom du modèle de point d'accès, ce qui rend très simple la tâche du pirate.

2° configuration du réseau sans fil

Dans la section concernant le paramétrage du réseau sans fil, il suffit de choisir les paramètres du réseau et de saisir un identifiant SSID caractérisant le réseau sans fil.

De préférence choisissez un SSID caractéristique, vous permettant d'identifier facilement votre réseau amis évitez d'y inclure des éléments d'informations personnelles (nom, prénom, adresse, etc).

Vous pouvez activer le service DHCP (Dynamic Host Configuration Protocol). Permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement (sans intervention particulière) sa configuration réseau. L'activation de ce service permet d'affecter automatiquement des adresses IP aux stations clientes. La plupart du temps il est possible de définir la plage des adresses attribuables, à l'aide d'une adresse de début, une adresse de fin et un masque de sous réseau.

3° Configuration des machines clientes

La configuration des machines clientes est très similaire à la configuration dans le cas d'un réseau d'égal à égal. Il suffit de cliquer sur l'icône de connexion réseau en bas à droite dans la barre système. Une fenêtre s'affiche.

Si un réseau est disponible à proximité, il est indiqué : cliquez sur le réseau du point d'accès, vous serez invité à saisir le mot de passe du réseau, puis si celui-ci est correct, vous êtes connectés au réseau.

Exercice

Installer et Configurer un réseau local mixte (filaire et sans fil)

SYSTEMES CLIENT-SERVEUR

Sortes des serveurs

Serveur des fichiers

Ces serveurs fournissent un espace centralisé, facilement partagé pour tous les ordinateurs du réseau, leur tâche essentielle est le stockage des fichiers et des programmes. Par exemple les clients du réseau peuvent utiliser l'espace de stockage du réseau pour y stocker leurs documents Microsoft office.

Les serveurs de fichiers doivent s'assurer que deux clients (utilisateurs) n'essayent pas de mettre à jour un seul fichier simultanément. Pour ce faire, les serveurs des fichiers verrouillent le fichier qui vient d'être ouvert et ne permettent qu'au premier utilisateur qui l'a ouvert de le modifier.

Serveur d'impression

Le partage d'imprimantes est l'une des principales raisons d'être des petits réseaux. Bien que cela ne soit pas une obligation, vous pouvez faire d'un ordinateur un serveur d'impression qui aura pour seule tache de collecter les données transmises par les ordinateurs et les imprimer dans un ordre préalable.

N.B. : un seul ordinateur peut faire l'objet serveur d'impression et d'un serveur des fichiers à la fois mais les performances seront meilleures si un ordinateur est réservé (dédié) à chacune de ces taches.

Serveur de messagerie

Le serveur de messagerie prend en charge la messagerie du réseau. Il est équipé de logiciels spécialisés comme Microsoft Exchange Server. Il doit être compatible avec le logiciel de messagerie. C'est le cas d'Exchange Server conçu pour fonctionner avec Outlook, la messagerie cliente fournie avec Office.

La plupart des serveurs de messagerie font vraiment plus qu'envoyer et recevoir du courrier électronique. Par exemple, voici quelques des fonctionnalités que MS Exchange server offre au-delà de simples courriers électroniques :

- Des conférences audio et vidéo ;
- Des formulaires personnalisés destinés à des applications telles que des demandes de congés ou des bons de commande.

Serveur web

Un serveur web est un ordinateur équipé de logiciels lui permettant d'héberger un site web, les plus connus sont IIS (Internet Information Services), de Microsoft et Apache, un programme Open source géré par Apache Software fondation.

Serveur de base de données

Un serveur de base de données est un ordinateur équipé d'un SGBD (Système de Gestion de Base de Données) comme MySQL server, Oracle, Mongo DB permettant de données accès aux bases de données qui y sont stockées.

Serveur d'application

Un serveur d'application est un serveur qui exécute une application spécifique. Par exemple, vous pouvez utiliser une application comptable qui exige son propre serveur dédié dans ce cas, vous aurez besoin d'affecter un serveur pour cette application.

Serveur DNS

Serveur de licences

Certaines organisations utilisent des logiciels qui nécessitent des licences à partir d'un serveur de licences centralisé. Par exemple, les entreprises d'aide d'ingénierie utilisent souvent des logiciels d'aide à la conception sur ordinateur (C.A.D) tels qu'AutoCAD Qui nécessitent un serveur de licences. Dans ce cas, vous aurez besoin de configurer un serveur pour gérer les licences et distribuer aux utilisateurs.

Serveur Proxy

Un serveur proxy (serveur mandaté ou proxy server) est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que TCP/IP) et internet.

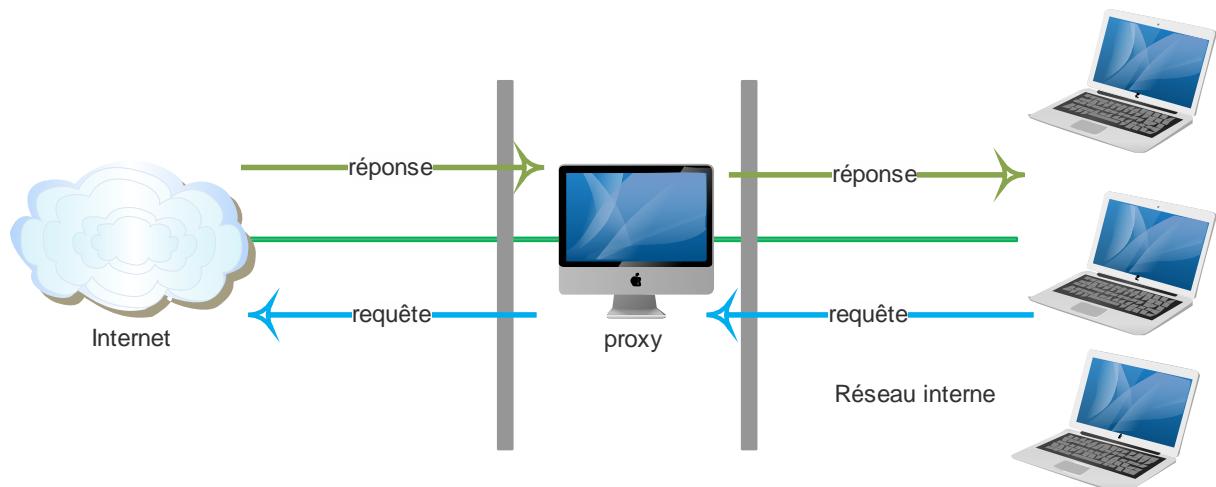
La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy http. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, etc.).

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur « mandaté » par une application pour effectuer une requête sur internet à sa place. Ainsi lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter au serveur et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche va lui transmettre la requête. Le serveur va ensuite donner la réponse au proxy, qui va à son tour la transmettre à l'application. Désormais avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par la passerelle et les routeurs. Pour autant les serveurs proxy sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités telles que le cache (filtrage et authentification) et reverse (relais inverse) : un serveur proxy-cache (monté à l'inverse) permettant aux internautes d'accéder indirectement à certains serveurs internes.

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur « mandaté » par une application pour effectuer une requête sur internet à sa place. Ainsi lorsqu'un utilisateur se connecte à internet à l'aide d'une application

client configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

Désormais avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Pour autant, les serveurs proxy sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités telles que le : **cache-proxy** (filtrage et authentification) et **reverse-proxy** (relais inversé), un serveur proxy-cache (monté à l'inverse), c'est-à-dire un serveur proxy permettant non pas aux utilisateurs d'accéder au réseau internet mais aux internautes d'accéder indirectement à certains serveurs internes.



Les systèmes d'exploitation serveurs

Définition

Un système d'exploitation réseau noté NOS, pour Network Operating System, est un système d'exploitation créé pour fonctionner en réseau sur le serveur. Il est constitué des fonctionnalités permettant la gestion d'un serveur. Dans un réseau où il y a plusieurs serveurs dédiés, il est préférable que les ordinateurs serveurs aient un seul système d'exploitation réseau identique comme par exemple :

- Le Windows serveur 2019 ;
- Linux, ou d'autres versions d'UNIX (Debian, UBUNTU)

Installation d'un serveur et partage de ressources

SECURITE INFORMATIQUE

La sécurité des systèmes d'information (SSI) est une discipline d'une importance première car le système d'information (SI) est pour toute entreprise un élément absolument vital, puisque le SI est vital, tout ce qui le menace est potentiellement mortel. Les menaces engendrent des risques et coût humaines et financiers : perte de confidentialité des données, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété. Ainsi l'ensemble de mesures prises pour éviter et prévenir ces menaces qui guettent un SI s'appelle sécurité information.

Définition des concepts

Sécurité des réseaux

La sécurité réseau est une sécurité informatique qui consiste à protéger le périmètre réseau.

Cybercriminalité

Elle est l'ensemble des infractions pénales s'exerçant au moyen du réseau internet.

Cyber attaque

Le cyber attaque est l'ensemble des attaques perpétrés par les cybercriminels sur les réseaux généralement internet.

Cyber sécurité

Est un ensemble de mesures sécuritaires prises contre le cyber attaque ; elle est une sécurité informatique dans le cyberspace (sur internet).

Hacking

Le hacking ou le piratage est une opération qui consiste à exploiter les vulnérabilités ou les failles de sécurité d'un SI pour dans le but de nuire (black hat hacker : pirate à chapeau noir) ou d'améliorer les mesures sécuritaire (white hat hacker ; pirate à chapeau blanc).

Cracking

Le cracking est la modification d'un produit commercial pour une utilisation non autorisée par le constructeur ou le distributeur officiel. Cracker un programme veut le soumettre à certaines opérations pour altérer les mesures de sécurité implantées par le constructeur afin de l'utiliser gratuitement ou le vendre.

La sécurité informatique peut être subdivisée en deux :

- La sécurité physique ;
- La sécurité logique.

Sécurité physique

La sécurité physique consiste à protéger l'infrastructure physique du SI. Toute protection logique est vaine sans sécurité physique convenable.

Pour assurer une bonne sécurité physique vous devrez attirer l'attention à ce qui suit :

- La qualité du bâtiment qui abrite les données et traitements à l'épreuve des intempéries, inondation, protégé contre les incendies et les intrusions, un contrôle d'accès adéquat.
- Qualité de l'alimentation électrique.
- Certification adéquat du câblage du réseau local des accès extérieurs.
- Pour l'utilisation de réseaux sans fil, placement méticuleux des bornes d'accès, réglage de leur puissance d'émission et contrôle des signaux en provenance et à destination de l'extérieur.
- Sauvegarde régulière des données sur des supports physiques adéquats distincts des supports utilisés en production.
- Transfert régulier des copies de sauvegarde en dehors du site d'exploitation.
- Aménagement d'un site de secours pour les applications vitales.

N.B. : ces solutions sont inopérantes si elles ne font pas l'objet d'une documentation tenue à jour et exercices périodiques.

Sécurité logique

La sécurité logique a pour mission de protéger le SI contre les menaces logicielles.

Elle protège le **Système d'exploitation** en configurant le droit d'accès : création, modification, destruction, lecture, et exécution des objets (fichiers et programmes). **L'authentification** : séparation des priviléges ou les priviléges minimums, le mot de passe et le chiffrement des données.

Malveillance informatique

Aujourd'hui quiconque navigue sur internet ou reçoit du courrier électronique s'expose aux logiciels malveillants (malware) que sont le virus, le vers et quelques autres que nous allons décrire, il importe que chacun acquière un minimum d'information sur ces logiciels :

Virus

Un virus est un logiciel capable de s'installer sur un ordinateur à l'insu de l'utilisateur légitime. Le terme virus est réservé aux logiciels qui se comportent ainsi avec un but malveillant parce qu'il existe des usages légitimes de cette technique dite **code mobile** : les appliquettes java et les procédures JavaScripts sont des programmes qui viennent s'exécuter sur votre ordinateur en se chargeant à distance depuis un serveur

web que vous visiter, sans que toujours vous en ayez conscience, et en principe le motif est légitime.

En général, pour infecter un système, un virus agit de façon suivante : il se présente sous forme de quelques lignes de code en langage machine (binaire) qui se greffent sur un programme utilisé sur le système cible, afin d'en modifier le comportement. Une fois implanté le greffon possède aussi en générale la capacité de se recopier sur d'autres programmes, ce qui accroît la virulence de l'infection et peut contaminer tout le système.

Botnet (virus réticulaire)

Le cible d'un virus informatique peut être indirecte : il y a des exemples de qui se propagent silencieusement sur des millions d'ordinateurs connectés à Internet sans y commettre le moindre dégât. Puis à un signal donné à une heure fixée, ces millions de programmes vont se connecter à un même serveur web, ce qui provoquera son effondrement. C'est ce qu'on appelle un déni de service distribué (**Distributed Denial of Service, DDoS**). Un tel virus s'appelle en argot SSI un **bot** et l'ensemble de ces virus déployés un **Botnet**. Les ordinateurs infectés par des bots sont nommés **zombies**.

Ver

Un ver (worm) est une variété de virus qui se propage par le réseau. Il peut s'agir d'un bot. En fait, alors qu'il des années les virus n'étaient pas de vers (ils ne se propageaient pas par le réseau) et le ver n'était pas de virus (il ne reproduisait pas), aujourd'hui la confusion entre les deux catégories est presque totale.

Cheval de Troie

Un cheval de Troie (trajan horse) est un logiciel qui se présente sous un jour honnête, utile ou agréable, et qu'une fois installé sur un ordinateur y effectue des actions cachées et pernicieuses.

Porte dérobée

Une porte dérobée (Backdoor) est un logiciel de communication caché, installé par un virus ou un cheval de Troie par exemple, qui donne à un agresseur extérieur accès à l'ordinateur victime par le réseau.

Bombe logique

Une bombe logique est une fonction cachée dans un programme en apparence honnête, utile ou agréable, qui se déclenchera à retardement, lorsque sera atteinte une certaine date, ou lorsque surviendra un certain événement. Cette fonction produira des actions indésirables, voire nuisibles.

Logiciel espion

Un logiciel espion comme son nom l'indique, collecte à l'insu de l'utilisateur légitime des informations au sein du système où il est installé, et les communique à un agent extérieur, par exemple au moyen d'une porte dérobée.

Une variété particulièrement toxique de logiciel espion est le **KeyLogger** (espion dactylographique), qui enregistre fidèlement tout ce que l'utilisateur tape sur son clavier et le transmet à son honorable correspondant ; il capte ainsi notamment identifiant, mots de passe et code secrets.

Spam ou courrier électronique non sollicité

Le courrier électronique non sollicité (spam) consiste en « communication électronique massives, notamment de courrier électronique sans sollicitation des destinataires à des fins publicitaires ou malhonnêtes ».

Les messages électroniques non sollicités contiennent généralement de la publicité, le plus souvent de la pornographie, des produits pharmaceutiques destinés à améliorer les performances du corps, des produits financiers ou des procédés d'enrichissement facile. Parfois il s'agit de l'escroquerie pure et simple, qui invite à accéder à leur site factice pour extorquer vos informations (numéro de téléphone, login et mot de passe) et cela s'appelle **phishing**.

Attaque sur le web

Injection SQL

Ces types d'attaques visent les sites web qui proposent des transactions mal construites utilisant les bases de données relationnelles. SQL est un langage qui permet d'interroger, de mettre à jour les données stocker dans une base de données relationnelle. Une requête typique est construite à partir des champs du formulaire remplis par l'internaute. Sans contrôle (vérification) des valeurs que l'internaute va insérer dans le formulaire cela constituera la faille de sécurité car un pirate pourra exploiter ces champs en confectionnant un texte tel qu'une fois incorporé à une requête SQL il ait des effets indésirables sur la base de données.

Par exemple sur le formulaire de connexion à une page web. Il est généralement utilisé cette requête : `requete = SELECT * FROM clients WHERE nom = ' ' + nom_client +'' ' and password = ' '' + mot_de_passe +'' '`

Un attaquant informé de cette faille, au lieu d'entrer dans le formulaire un mot de passe valide, introduit la chaîne des caractères suivants : `x' ; DROP TABLE Clients` ; la requête sera : `requete = SELECT * FROM cleints WHERE nom ='' AND Password = 'x' ; DROP TABLE clients` ; avec comme résultat, la destruction pure et simple de la table client.

La parade à ce type d'attaque consiste à écrire des programmes moins naïfs, qui vérifient les données introduites par l'utilisateur avant de les utiliser, et en particulier en éliminant les caractères qui ont une valeur sémantique spéciale pour SQL.

Cross-site-Scripting

Ces types d'attaques sont apparus avec le langage JavaScript. Elle consiste à injecter dans une page HTML sur le web un programme qui viendra s'exécuter dans le navigateur de l'internaute à son insu. Ces actions risquent d'être peu désirables, mais surtout elles peuvent rediriger discrètement le navigateur vers un site malveillant qui pourra injecter du code dans la page visitée.

Il convient de ne pas sous-estimer les risques induits par ce genre de faille, par exemple si la page détournée comporte des demandes d'authentification avec mot de passe ou des transactions financières.

Palimpsestes électroniques

Palimpseste électronique est une technique qui consiste à utiliser un document dans un lecteur spécialisé pour voir l'historique de modification à des fins malicieux ou de curiosité.

Matériel de rebut

Quand vous mettez votre ordinateur au rebut, assurez-vous d'avoir effacé sainement le contenu de votre disque. Le pirate peut acheter des disques durs au rebut pour trouver des informations confidentielles, des cartes de crédit et autres.

Risque liés au réseau sans fil

Les risques liés à la mauvaise protection d'un réseau sans fil sont multiples :

- Interception des données : consistant à écouter les transmissions des différents utilisateurs du réseau sans fil ;
- Détournement de connexion : le but est d'obtenir l'accès à un réseau local ou internet ;
- Brouillage des transmissions : consistant à émettre des signaux radios de manière à produire des interférences ;
- Denis de service : rendant le réseau inutilisable en envoyant des commandes factices.

Pour éviter ces problèmes plusieurs solutions sont proposées :

- Utilisation d'une infrastructure adaptée pour assurer la portée du réseau dans fil ;
- Filtrages des adresses MAC ;
- Utilisations des protocoles WEP (Wired Equivalent Privacy) pour assurer la confidentialité des communications ;
- Améliorer l'authentification en utilisant WPA ou le serveur Radius ;
- Utilisation des VPN.

Luttes contre les malveillances informatiques

Face aux menaces informatiques : virus, ver, cheval de Troie et autres, différents outils capables de dépister les différentes catégories de maliciels et éliminer tout danger potentiel existent parmi lesquels :

Antivirus

Les antivirus sont des programmes destinés à protéger un S.I. des virus informatiques. Ils peuvent principalement s'installer en deux sortes d'endroits :

1. Soit à l'entrée du réseau, là où arrive les flux en provenance de l'internet ; certains de ces flux seront filtrés pour y détecter des virus ;
2. Soit sur le poste de travail de l'utilisateur, et là l'antivirus servira généralement à inspecter et désinfecter le disque dur.

N.B. : gardez à l'esprit que certains virus s'exécutent en mémoire vive, sans s'enregistrer sur le disque.

Mode de fonctionnement des antivirus

Il y a essentiellement deux (2) modes de fonctionnement des antivirus :

1. Mode statique : le logiciel est activé sur ordre de l'utilisateur, par exemple pour déclencher une inspection du disque dur ;
2. Le mode dynamique : le logiciel est actif en permanence et scrute certains événements qui surviennent dans le système.

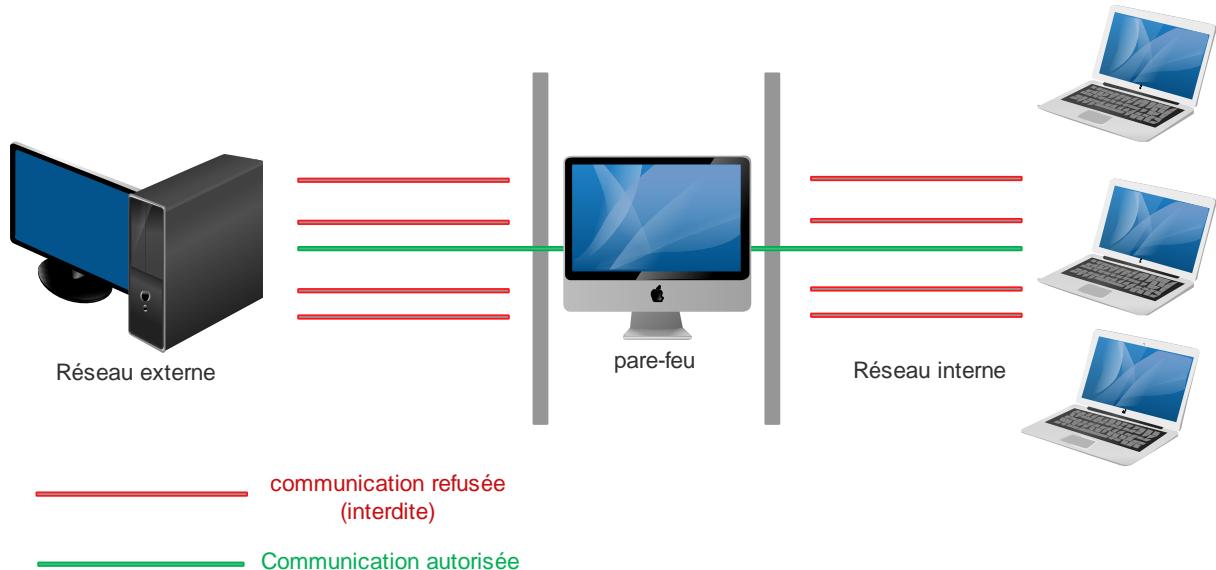
Quelques antivirus

De nombreux antivirus sont disponibles sous forme **des produits commerciaux** (norton, Kaspersky, AVK, F-Secure, etc.) ou de **shareware** (Avira, Avast, AVG, Antir Personnel Edition, etc.). certains étant parfois installés dans le Kit logiciel qui accompagne un ordinateur neuf.

N.B. : la plupart de ces produits sont incompatibles entre eux, il ne faut jamais installer deux (2) antivirus différents sur un poste.

Pare-feu

Un pare-feu (coupe-feu, garde barrière ou firewall) est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers.



Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la communication (Allow) ;
- De bloquer la communication (Deny) ;
- De rejeter la connexion sans avertir l'émetteur (Drop).

L'ensemble de ces règles permettent de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité permettant :

- D'autoriser uniquement les communications ayant été explicitement autorisées « tout ce qui n'est pas explicitement autorisé est interdit » ;
- Soit d'empêcher les échanges qui ont été explicitement interdits ;

N.B. : il y a plusieurs types de filtrages qu'il est possible d'utiliser avec un firewall : **filtre simple** (adresse Ip, Port), **dynamique** (inspection au niveau de la couche 3 et 4 du modèle OSI), **filtrage applicatif** (inspection au niveau de la couche 7, on parle de passerelle applicative ou proxy) **et pare-feu personnel** (pour chaque ordinateur du réseau).

Exercice

Configurer et paramétrier un serveur local pour le partage des ressources (données imprimantes)

RESEAUX SOCIAUX

Concepts de base

Réseau social

Pour comprendre le mot réseau social il est important de définir chacun de mots qui le contient : réseau et social.

Réseau : ce mot vient du latin **retis** qui signifie filet, le mot réseau à plusieurs définitions :

Selon le dictionnaire la rousse :

Ensemble formé de lignes ou d'éléments qui communiquent ou s'entrecroisent.

Ensemble de routes, de voies navigables, de lignes aériennes ou chemin de fer, qui relient différentes régions entre elles, qui appartiennent à une même compagnie.

Selon le robert :

Ensemble de voies, de canalisations, de conducteurs reliés les uns aux autres : réseau routier.

Dans chacune de ces définitions il y a l'aspect *liaison (relier)* et *communication* qui sont repris. Donc un réseau permet de relier plusieurs entités (personnes, zones) et cette liaison permet la communication.

Social, vient également du latin **socius** qui signifie « associés », l'adjectif social a plusieurs définitions :

Qui se rapporte à une société, une collectivité humaine comme entité propre.

Qui a un rapport avec la société, qui la caractérise : vie sociale, morale sociale.

Dans chacune de ces définitions le mot social fait appel toujours à la société.

Par définition le réseau social est un site web proposant de créer un réseau relationnel et offrant des services à ses membres pour fédérer ce réseau. Il s'agit d'un site qui propose de créer un réseau relationnel (maillage en quelque sorte) autour de vous et le reste du monde.

Média social désigne quant à lui l'ensemble de sites et d'outils sociaux du web. Un média social est un procédé permettant la distribution ou la diffusion de documents, contenus sonores ou visuels. La frontière entre média et réseau social est donc mince. Par exemple Facebook est à l'origine un réseau social dont la puissance en fait un média social incontournable.

Identité numérique

Chaque personne possède une identité dans la vraie vie. Avec l'avènement high-tech et plus précisément du web et des réseaux sociaux on parle désormais aussi d' « identité numérique » : ce terme désigne **l'ensemble des données concernant une personne éparses sur internet** : des données des publications diverses (statuts, liens, photos, vidéos, commentaires, etc.). Sur les réseaux sociaux, les blogs, les sites de partage, des avis consommateur et même les scores obtenus à des jeux vidéo. Cette identité englobe à peu près tout ce que vous faites sur internet (web) et qui laisse une trace : ce que vous exprimez, partez, consommez, appréciez ou au contraire de critiquer, vos coordonnées personnelles (C.V., profil sur le réseau professionnel, votre réputation : avis laissés par d'autres internautes sur vous, par exemple sur stackoverflow), vos loisirs, vos connaissances (articles) sur Wikipédia, vos relations (personnes suivies sur twitter ou Instagram par exemple, amis sur les réseaux sociaux, etc.), la musique que vous écoutez, les films que vous voyez, les lieux que vous fréquentez (et pour lesquelles vous utilisez un outil de partage de géolocalisation).

En fait, l'identité numérique est **l'ensemble de traces que vous laissez sur internet.**

Sécurité et Confidentialité sur les réseaux sociaux

La confidentialité est l'ensemble d'outils qui vont vous permettre de rendre vos contenus privés ou publics ; elle permet de sauvegarder votre vie privée sur les réseaux sociaux.

Quel que soit le réseau social, la confidentialité et la sécurité de vos données, de votre image et de vos propos sont des sujets cruciaux. Ce qu'il faut retenir tient en quelques points essentiels :

- Il est possible de contrôler la diffusion de manière précise pour la plupart des informations confiées aux réseaux sociaux, grâce aux paramètres de confidentialité. En cas de problème, vous pouvez bloquer une personne.
- Tout ce que vous publiez ou partagez, même avec des paramètres de confidentialité restreints vous engage : ne diffusez pas des propos ou photos qui constituent un délit de quelque ordre. Un utilisateur peut ainsi signaler une publication qui lui semble abusive.
- Vous devez respecter la propriété intellectuelle, le droit d'auteur et le droit à l'image. Par exemple ne copier pas la photo de profil ou le statut de votre ami sans aval.

Vous devez respecter les conditions d'utilisations du réseau social dans lequel vous faites partie.

Types de réseaux sociaux

On dénombre près de 700 réseaux sociaux en tout, dans le monde entier. Il en apparaît et disparaît d'ailleurs à chaque instant. On peut classer les réseaux sociaux par types selon l'**usage** qu'en font leurs membres, mais aussi selon leur **nature sociale** :

Par objectif (usage) : On distingue plusieurs grands types d'usage des réseaux sociaux :

- Partager, agréger du contenu : ces réseaux permettent de partager du contenu vidéo, photo, sons, essentiellement créé par l'utilisateur ou non

Exemple : Youtube, Vimeo, Flickr, Myspace, Pinterest, scoop.it

- Publier et s'exprimer : ces plateformes permettent de produire et diffuser simplement un contenu, sous la forme d'articles, aussi appelés « posts » ce sont des blogs et les wiki.

Exemple : Twitter, Google+, Tumblr, WordPress, Wikia.

- Réseauter et collaborer : c'est l'objet premier des réseaux professionnels, qui permettent la mise en relation de collaborateurs ou de rassembler une communauté d'employés d'une même entreprise.

Exemple : LinkedIn, Viadeo, Glassdoor, Yammer.

- Se localiser : ils permettent aux utilisateurs de partager leur position géographique ou la visite d'un lieu, signaler leur présence dans des lieux à leurs amis ou à la communauté et gagner des points.

Exemple : fourquare, swarm, Yelp.

- Faire de rencontre : permettent aux utilisateurs de rencontrer l'amour (ou au moins essayer) ou se faire des amis.

Exemple : Tinder, Happn, Once, Lovoo.

- Jouer : ils permettent aux membres de fédérer un ou plusieurs jeux video.

Exemple : Twitch, PlayFire.

Selon la nature sociale Nous avons :

- Les réseaux sociaux personnels : placent l'utilisateur au centre de leurs fonctionnalités. En lui permettant de partager le contenu personnel ou ayant un intérêt particulier.

Exemple : Google+, Fourquare.

- Les réseaux sociaux de partage de contenus : orienté vers le partage de contenus personnels ou non c'est-à-dire produit par d'autres utilisateurs.

Exemple : Twitter, Instagram, YouTube, Pinterest, Spotify.

- Les réseaux sociaux ciblés sur les intérêts communs : sont très orientés « communauté » et ont une nature informative, fondée sur les intérêts à la fois personnels et professionnels :

Exemple : LinkedIn, Viadeo, GlassDoor, Quora, Ask, Yahoo ! Question/Réponse, TripAdvisor.

NB. : le plus célèbre des réseaux sociaux n'est pas cité dans la plupart des exemples : Facebook, il se trouve à la croisée de plusieurs de ces familles et offre des fonctionnalités appartenant à nombre d'entre elles. C'est un réseau généraliste.

Voici les réseaux sociaux ou communauté en ligne ayant plus de 100 millions d'utilisateurs actifs. Cette classification a été tiré du livre de YASMINA SALMANDJEE et Paul DURANT DEGRANGES « **les réseaux sociaux pour les nuls** ».

| Nom | Membres inscrits | Utilisateurs actifs | Pays d'origine |
|---------------------------|-------------------------|----------------------------|-----------------------|
| Facebook | 2+ milliards | 1,49 milliards | Etats-Unis |
| WhatsApp | 900+ millions | 900 millions | Etats-Unis |
| Tencent QQ | 1+ milliards | 843 millions | Chine |
| Facebook messenger | 2+ milliards | 700 millions | Etats-Unis |
| Tencent Q Zone | 1+ milliards | 650 millions | Chine |
| WeChat | 1+ milliards | 600 millions | Chine |
| Google+ | 2+ milliards | 540 millions | Etats-Unis |
| Instagram | 400+ millions | 400 millions | Etats-Unis |
| Twitter | 1+ milliards | 304 millions | Etats-Unis |
| Skype | 663+ millions | 300 millions | Estonie |
| Baidu Tieba | 1 milliard | 300 millions | Chine |
| Viber | 606 millions | 249 millions | Israël |
| Sina Weibo | 503+ millions | 212 millions | Chine |
| LINE | 600 millions | 211 millions | Japon |
| YY | 773 millions | 122 millions | Chine |
| Snapchat | 100+ millions | 100+ millions | Etats-Unis |
| Pinterest | 100+ millions | 100 millions | Etats-Unis |
| BBM | 160 millions | 100 millions | Canada |
| LinkedIn | 380 millions | 97 millions | Etats-Unis |

Avantages d'utiliser les réseaux sociaux

De manière générale l'avantage d'utiliser les réseaux sociaux de communiquer avec ses contacts. Autrement dit : fédérer avec sa communauté d'amis et garder contact, échanger avec sa famille, entretenir de bonnes relations professionnelles, etc.

Des nombreux aspects des réseaux sociaux rendent très pratique leur utilisation : annoncer une nouvelle à tous ceux que vous connaissez, partager les photos de vos dernières vacances, mettre à jour son C.V. en ligne, etc.

L'emploi des réseaux sociaux peut aussi être plus intéressant : obtenir l'aide pour trouver un appartement grâce au bouche à oreille ou trouver un emploi, faire de la publicité pour votre entreprise par exemple.

Problème lié à la sécurité sur les réseaux sociaux

Il y a plusieurs problèmes ou inconvénients liés à l'utilisation multiple des réseaux sociaux : le désir d'être présent et de manière active sur bon nombre d'entre eux. Des telles activités demandent plus de temps et d'organisation surtout qu'il s'agit souvent de publier les mêmes informations d'un compte à l'autre. Sans oublier le temps passé entant que spectateur sur ces réseaux. Donc l'utilisation intensive des réseaux sociaux peut vite devenir chronophage.

L'utilisation très intensive des réseaux sociaux peut conduire à des dérives : démotivation, isolement, perte de repères, exposition au harcèlement (surtout les jeunes filles) sont des dangers qui guettent les accros de ces sites.

Les vols des informations des informations d'authentification du compte sont aussi courants.

Ethique et morale et observer

Le monde a déjà beaucoup de problème en ajouter serait une erreur. Etant qu'utilisateur des réseaux sociaux vous devez respecter les règles de la morale et la politique de confidentialité du réseau :

- N'est pas publier des fake news pour se faire intéressant ;
- Respecter les règles et la politique de confidentialité du site web utilisé ;
- Respecter le droit d'auteur ou la propriétaire intellectuelle. J'ai déjà vu une personne prendre une vidéo sur le statut de son ami sans demander et la sauvegarde sur son téléphone ;
- N'espionnez pas vos amis. J'ai déjà vu un utilisateur de Facebook créer un compte similaire à compte d'une fille pour essayer de dérouter les amis de la fille et essayer de faire passer pour elle.

En bref, entant que membre d'un réseau social vous devez respecter la vie privée des autres.

Exercice

Création d'une plateforme (groupe) sur les réseaux sociaux, de définir la charte (WhatsApp, Facebook)

INTELLIGENCE ARTIFICIELLE

Concepts de base

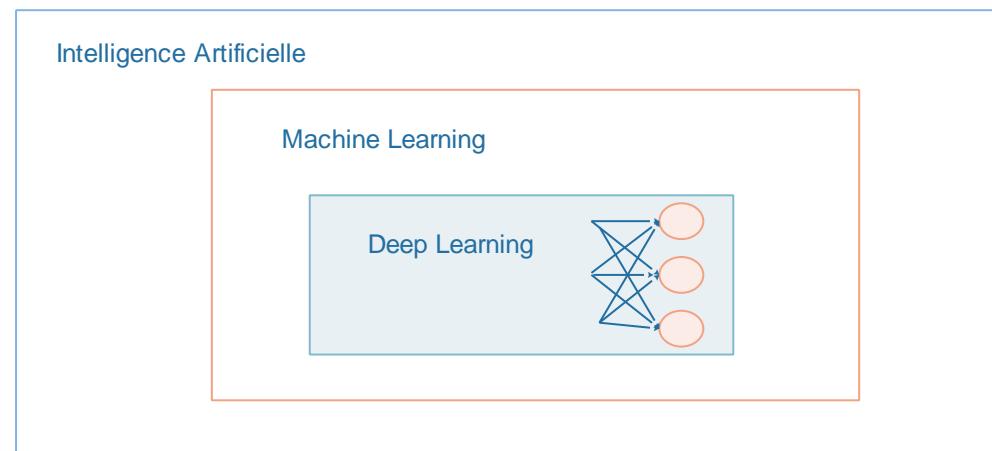
Intelligence artificielle

Le terme « intelligence artificielle » créé par **John MCCARTHY**, est souvent abrégé par le sigle « I.A. » ou « A.I. » en anglais pour **Artificial Intelligence**. Elle englobe un ensemble des théories et techniques mises en œuvre en vue de réaliser des machines capable de simuler l'intelligence humaine.

Marvin Minsky défini l'I.A. comme étant science dont le but est de faire réaliser par une machine des tâches que l'homme accomplit en utilisant son intelligence.

Pour y parvenir nous avons besoin d'apprendre à notre machine comment réaliser ces tâches par le biais **d'algorithme conçus à partir de modèles statistiques**. C'est ce qu'on appelle **Machine Learning**.

Le Deep Learning est quant à lui une branche du Machine Learning s'appuyant sur l'usage **des neurones artificiels** (Yan Le Cun) s'inspirant du cerveau humain. Ces neurones sont organisés en couches donnant alors une notion de **profondeur** (Deep) au réseau de neurones. Par conséquent lorsque nous parlons d'intelligence artificielle, il est préférable de parler de Machine Learning ou de Deep Learning



Apprentissage artificiel/automatique ou machine

Le machine Learning ou l'apprentissage automatique est l'ensemble d'outils statistiques ou géométriques et d'algorithmes informatiques qui permettent d'automatiser la construction d'une fonction de prédiction f à partir d'un ensemble d'observation que l'on appelle **ensemble d'apprentissage**. Le machine Learning est donc une discipline hybride entre plusieurs sciences et techniques que sont l'analyse statistiques, l'intelligence artificielle, la bio-information et l'IT.

Les différents types d'apprentissage

Une machine capable d'apprendre selon trois formes d'apprentissages :

1. Le premier est l'apprentissage dit supervisé

C'est-à-dire que la machine va apprendre à partir de données labellisées par l'être humain. Par exemple dans le cas de reconnaissance d'image entre un chat ou chien, pour chaque image utilisée dans l'apprentissage nous devons indiquer à la machine s'il s'agit d'un chat ou d'un chien. Cette indication s'appelle **labellisation**.

2. Vient ensuite l'apprentissage non supervisé

Dans ce cas, la machine va apprendre (seule) par elle-même. Mais le terme d'apprentissage autonome reste très appellatif. La machine est capable de faire des regroupements et donc de réaliser des classifications, cependant elle n'est pas capable de définir par elle-même les différents libellés, car elle n'a conscience des données dont elle a la charge d'en apprendre.

3. Enfin, l'apprentissage par renforcement

Cet apprentissage consiste pour la machine à apprendre par l'expérience et étant récompensé de façon positive ou négative en fonction des décisions.

Big data

Depuis le début de l'informatique personnelle dans les années 1980, jusqu'à l'omniprésence du web actuelle dans la vie de tous les jours, les données ont été produites en quantité toujours croissante : photos, vidéos, sons, textes, log en tout genre... depuis la démocratisation de l'internet ce sont des volumes impressionnantes des données qui sont créées (déluge de données) quotidiennement par les particuliers, les entreprises et maintenant les **objets et machines connectées (IOT)**.

Le terme « Big Data » littéralement traduit par « grosses données » ou « données massives » désigne cette explosion des données. On parle généralement de « data masse » en analogie avec la biomasse, écosystème complexe et de large échelle.

Cette hausse de la *consommation de services informatiques se traduit mécaniquement par une demande croissante de puissance de traitement et de stockage de données* qui engendre une obsolescence des architectures IT habituellement utilisées : base de données relationnelles et serveurs d'applications doivent laisser la place à des solutions nouvelles.

Face aux nouvelles exigences de la montée en charge et la disponibilité, une nouvelle classe de système de **bases de données non relationnelles** a émergé. On désigne habituellement ces systèmes au moyen du sigle NoSQL (Not only SQL) pour traiter ce volume colossal des données. Des modèles de traitement parallèles des données ont également vu le jour avec des algorithmes innovants comme **MapReduce de Google**, des outils comme **Hadoop Apache** pour la communauté Open Source, des langages de transformation et de requête **Pig et Hive**.

Base de données NoSQL

Que veut dire le sigle « NoSQL » ? Le moins que l'on puisse est que cette dénomination ne désigne pas exactement ce que sont ces bases de données. Pour certains, le « No » ne voudrait pas forcément dire « no », il pourrait signifier aussi « Not only, la partie

« SQL » est très trompeuse encore puisque ce n'est pas l'absence du langage SQL qui est plus significative pour beaucoup de ces systèmes, mais l'absence de transactions au sens usuel du terme. En réalité ce sigle n'a pas été choisi à des profondes réflexions conceptuelles. Il s'agit d'un simple hashtag utilisé en 2009 pour notifier l'organisation d'un débat à San Francisco sur ces bases de données d'un nouveau genre.

Voici quelques préoccupations auxquelles répondent ces genres de bases de données :

- Distribuer les traitements et le stockage sur des centaines voire des milliers de nœuds constitués des serveurs banalisés ;
- Données la priorité aux performances et à la disponibilité sur l'intégrité des données ;
- Traiter efficacement les données non structurées ou partiellement structurées.

Bien qu'une définition honnête soit impossible, il est possible néanmoins d'identifier certains **points communs** à ces systèmes :

- Ces systèmes sont les plus souvent clusterisables et permettent la montée en charge *approximativement linéaire*. En d'autres termes, un doublement du nombre de serveurs permet, grossièrement, de traiter deux fois plus de requêtes dans même laps de temps ;
- Ils sont en règle générale dépourvus de schémas ; inadaptés aux données aux données structurées, cette caractéristique leur confère un atout significatif vis-à-vis des bases de données relationnelles : ils permettent une grande rapidité de développement précisément adaptées aux méthodologies agiles ;
- Ils sont dépourvus des transactions au sens habituel du terme, ou alors proposent de transactions qui garantissent seulement l'intégrité de certains agrégats de données naturelles ;
- Ils sont non relationnels dans la mesure où ils n'offrent pas de jointures.

Les différentes catégories des bases de données NoSQL

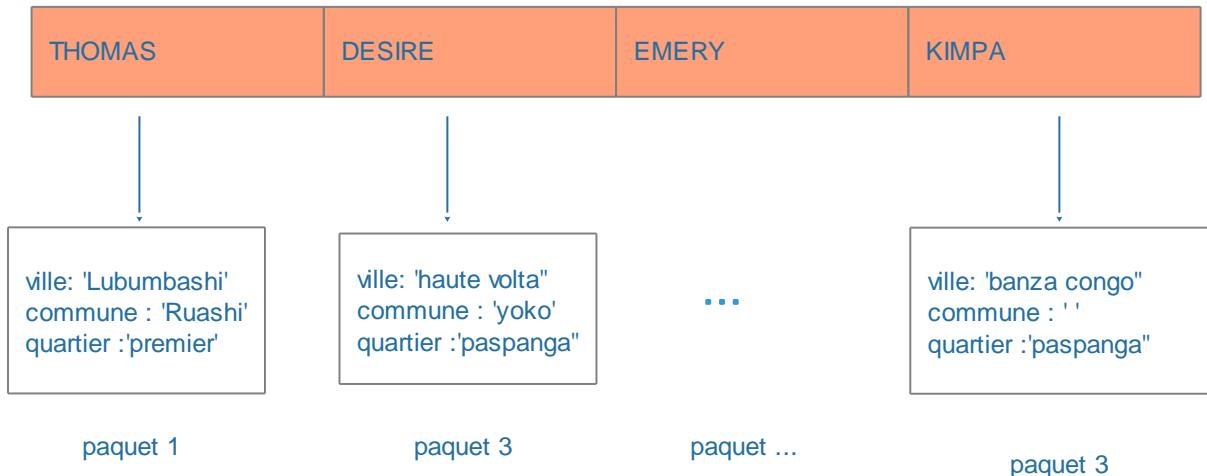
Pour illustrer les catégories de base de données NoSQL nous allons utiliser une table de départ d'une base de données relationnelle à partir de laquelle nous essayerons de représenter sous forme NoSQL pour chacune de catégories.

| Id | Ville | commune | Quartier |
|-----------|--------------|----------------|-----------------|
| THOMAS | Lubumbashi | Ruashi | premier |
| DESIRE | Haute volta | Yoko | Paspanga |
| EMERY | | Ruashi | premier |
| KIMPA | Banza Congo | | paspanga |

Les bases de données NoSQL sont classées en quatre (4) catégories :

1. Bases de données orientée clé-valeur

Utilisées pour leur efficacité et leur facilité de mise en œuvre ; elles consistent à créer une table de hashtag pour chaque entrée d'une base de donnée relationnelle.



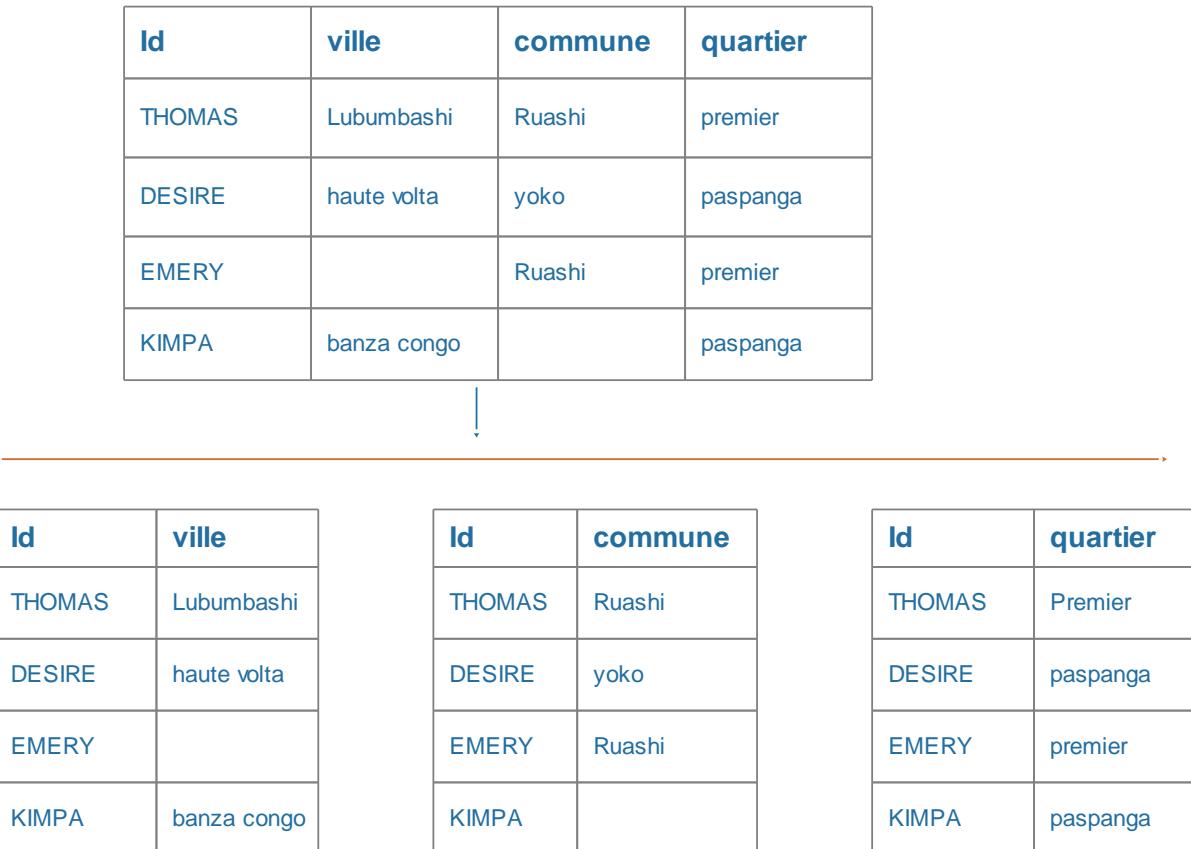
Exploitées grâce aux opérations de type CRUD (Create, Read, Update et Delete)

Parmi les bases de données orientées clé-valeur nous avons :

- Redis ;
- Amazon SimpleDB ;
- Microsoft Azure ;
- MemCached.

2. Bases de données orientées colonne

Elle exploite la structure, elle consiste à découper chaque attribut en un ensemble des colonnes que l'on va pouvoir distribuer sur l'ensemble des serveurs en y associer à chaque fois la clé primaire.



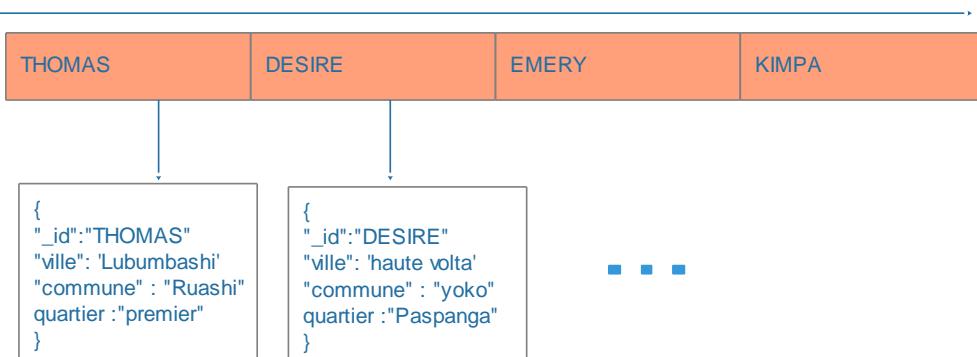
Parmi les bases de données orientées colonnes nous avons :

- BigTable
- Apache HBase
- ElasticSearch
- SparkSQL

Utilisée pour faire les agrégations afin de créer de corrélations entre les colonnes dans l'objectif de constituer un résultat agrégé.

3. Les bases de données orientées document

Elles reprennent le concept de clé, la notion de table de hachage (hashtag), mais au lieu d'avoir un paquet brut on va avoir un document à l'intérieur ayant une structure bien particulière exploitable par la base de données.

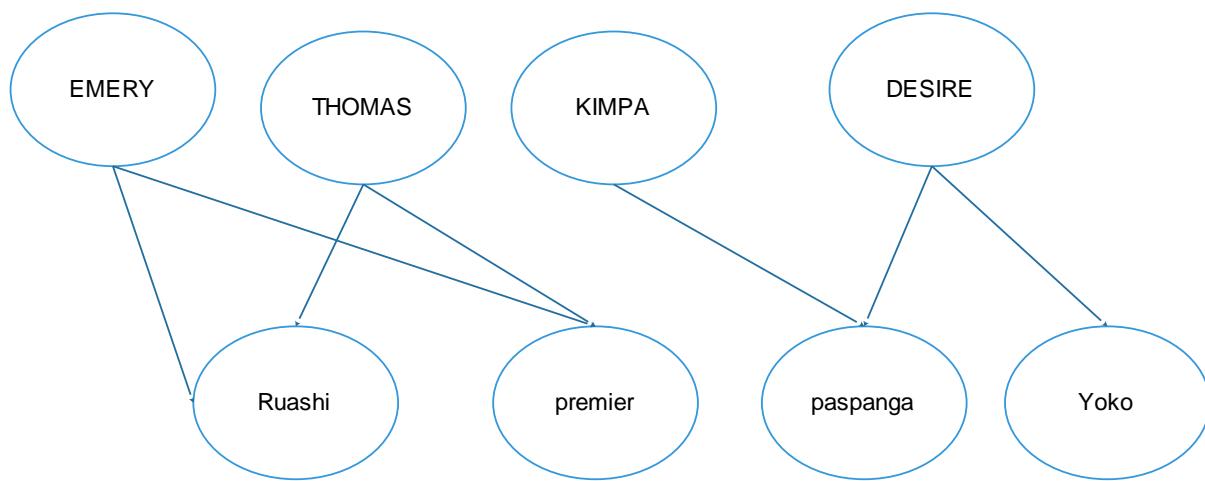


Elles sont utilisées pour leurs requêtes riches et la gestion d'objet. Parmi ces bases de données nous avons :

- Couch Base
- MongoDB
- Cassandra de Facebook
- DynamoDB

4. Les bases de données orientées graphes

Elles permettent d'exploiter la forte corrélation qu'il y a avoir entre les données. Par exemple pour notre table de données on peut prendre les identifiants pour former les noeuds que l'on doit pouvoir enrichir avec des propriétés et puis les communes et les quartiers.



On obtient donc un graphe que l'on doit pouvoir interroger avec des requêtes de haut niveau. Ces systèmes sont utilisés pour les exploitations des réseaux sociaux, des recommandations d'amis, ... parmi les bases de données orientées graphes nous avons :

- Neo4J
- Azure Cosmos DB
- Orient DB
- Flock DB

N.B. : - les bases de données NoSQL sont conçus pour répondre au théorème le CAP : **Consistency** (cohérence), **Availability** (Disponibilité) et **Partition** tolerance (tolérance aux pannes ou distribution).

- elles sont associées au **sharding**, qui est une technique qui permet de découper un fichier en plusieurs bouts repartis intelligemment sur le réseau en utilisant la répartition et les techniques d'indexation (HDFS).

Domaines d'application de l'intelligence artificielle

Finances et banques

Certaines banques font appel à l'IA et développent des systèmes experts de l'évaluation de risque lié à l'octroi d'un crédit (credit-scoring).

Militaire

Le domaine militaire utilise des systèmes tel que : les drones, les systèmes de commandement et d'aide à la décision.

L'utilisation de l'IA dans le domaine militaire est devenue de plus en plus important. Plusieurs projets d'armement basés sur l'IA sont en cours de développement. Par exemple, la France avec CCIAD (cellule de coordination de l'IA de défense), les états unis avec MAVEN,...

Médecine

La médecine a aussi de grands progrès grâce à l'utilisation des systèmes d'aide au diagnostic ou diagnostic automatique.

Renseignement policier

Un usage de l'intelligence artificielle se développe dans la prévention des crimes et délits.

Droit

Le droit fait appel à IA dans la perpective de prédire les décisions de justice, d'aide à la décision et de trancher des cas simples.

Logistique et transports

Le domaine de la logistique a vu certains projets utilisant de l'intelligence artificielle se développer pour la gestion de la chaîne logistique (supply chain) ou des problèmes de livraison telle celle du dernier kilomètre. Elle est également utilisée dans le domaine de transport en commun, car elle permet de faciliter la régulation et la gestion du trafic au sein d'un réseau de plus en plus complexe.

Industrie

Les systèmes intelligents deviennent monnaie courante dans de nombreuses industries. Plusieurs tâches peuvent leur être confiées, notamment celles considérées comme trop dangereuses pour un humain. Certaines applications se concentrent sur les systèmes de maintenance prédictive, permettant des gains de performance grâce à une détection des problèmes en amont.

Robotique

La robotique à recours à l'intelligence artificielle à plusieurs égards. Notamment pour la perception de l'environnement (objets et visages), l'apprentissage et l'intelligence artificielle développementale.

Jeux vidéo

L'IA est par exemple utilisée pour animer les personnes non-joueuses de jeux vidéo, qui sont conçus pour servir d'opposants, d'aide ou compagnons lorsque des joueurs humains ne sont pas disponibles ou désirés. Dans jeux à deux joueurs où l'on utilise des algorithmes **Minimax**, **alpha-beta**,...

Art

Dès la fin des années 1980, des artistes s'emparent de l'IA pour donner un comportement autonome à leurs œuvres.

Autres domaines

La domotique, avec des robots employés de maison, ou pour certaines tâches précises comme domotique, en programmation, journalisme, et design...

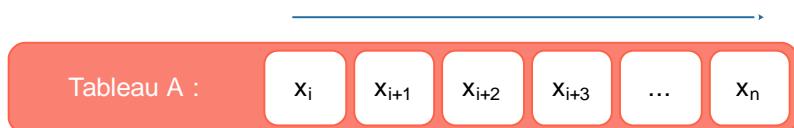
Création des ordinogrammes et des algorithmes simples

Algorithme de recherche

Un algorithme de recherche permet de rechercher une valeur dans une collection de données (tableau). Il y a plusieurs manières de rechercher une valeur dans une collection :

1. La recherche linéaire

La recherche linéaire est à la manière la plus élémentaire de rechercher une valeur dans un tableau en parcourant celui-ci de l'élément à l'indice i jusqu'à l'élément à l'indice n . Avec la recherche linéaire nous parcourons le tableau qui contient les éléments de la première jusqu'à l'extrémité droite.



Dans ce cas il faut utiliser une boucle pour parcourir les éléments comme suit :

```
Pour i = 1 à n faire
    // La recherche se fera ici
Fin pour
```

A chaque itération on essayera de comparer si la valeur recherchée (x) correspond à l'élément du tableau à l'indice i , ce qui donne la procédure suivante :

Procédure Recherche-Linéaire (A, x, n)

A : est un tableau des éléments
 X : est l'élément recherché
 n : est le nombre d'élément de A

Variable réponse = -1

Début

Pour i = 1 à n faire la chose suivante

Si A[i] = x alors

réponse = i

Fin si

Fin pour i

Retourner réponse

Fin

Notre procédure recherche-linéaire commence par créer une variable réponse à laquelle on affecte la valeur -1, pour signifier que jusque-là nous n'avons pas encore trouvé l'indice de l'élément recherché. Ensuite on parcourt le tableau A en commençant par la première indice $i=1$ jusqu'à l'indice n . et à chaque itération nous essayons de comparer la valeur se trouvant à l'indice i à x comme suit Si $A[i] = x$ alors, dans l'affirmative on affecte l'indice i à la variable réponse. Après le parcours de notre boucle, la procédure retourne la contenu de la variable réponse.

Attention la plupart des langages de programmation utilise [0] pour le premier élément d'une collection.

Avec notre procédure, imaginer si x correspondait à la valeur de la première case, notre boucle continuera le parcours en d'autre terme la recherche linéaire continue à parcourir le tableau même si l'élément recherché est trouvé, ce qui est une perte de temps inutile.

Normalement lorsque vous recherchez le roman « le haut et le bas » de ZAMENGA dans votre étagère, une fois trouvé vous ne continuerez pas à rechercher à moins à moins que vous ayez pris une bouteille de « LUTUKU ». Donc nous allons optimiser notre procédure linéaire afin qu'elle stoppe son traitement dès qu'elle a trouvé la valeur x dans le tableau.

Procédure Meilleure-Recherche-Linéaire (A, x, n)

A : est un tableau des éléments
 X : est l'élément recherché
 n : est le nombre d'élément de A

Début

Pour i = 1 à n faire la chose suivante

Si A[i] = x alors

```

        Retourner i
    Fin si
Fin pour i
Retourner -1
Fin

```

Je crois qu'il faut peut-être expliquer l'optimisation dont il est question, dans la nouvelle procédure il y a présence l'instruction `Retourner i` dans la boucle, cette instruction a pour effet de quitter la boucle une fois que $A[i] = x$.

Nous venons de donner précédemment deux variantes de la recherche linéaire. Une question vient à l'esprit « pouvons-nous faire mieux ? » cela dépend, si le tableau est trié ou pas.

N.B. : la recherche linéaire à temps d'exécution qui dépend de n ou $\theta(n)$ c'est-à-dire de la taille du tableau, Plus grand est le tableau, plus long est le temps d'exécution mais le temps d'exécution est $\theta(n)$ dans le cas le plus défavorable car dans le cas favorable (par exemple l'élément recherché se trouve à l'indice 0 ou 1), le temps d'exécution est $\theta(1)$. Si vous voulez aller plus loin et comprendre les notations sur le temps d'exécution des algorithmes, consultez le livre : « Algorithmes, notions de base » de Thomas H. Cormen. Publié aux éditions DUNOD.

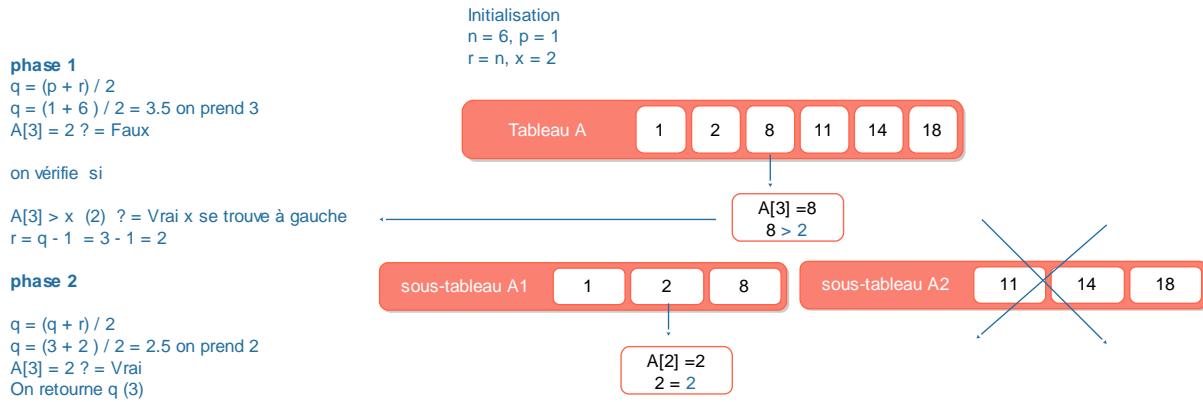
2. La recherche dichotomique

La recherche dichotomique ou binaire consiste à rechercher un élément dans un tableau des éléments triés dont chaque élément est inférieur ou égale à son successeur. Pour un élément que signifie être inférieur ou égal ? Lorsque les éléments sont des nombres, le sens est évident. Lorsque les éléments sont des chaînes de caractères, nous pouvons imaginer un **ordre lexicographique** : un élément est inférieur à l'autre s'il vient avant celui-ci dans le dictionnaire. Lorsque les éléments sont des données d'autres formes, nous devons donner la définition de « inférieur ou égal » tant qu'elle est claire, nous déterminer si le tableau est trié. Pour faire une recherche dichotomique le tri est une étape préalable.

Cette recherche exige un tableau trié, son avantage est le temps d'exécution $\theta(\lg n)$.

Imaginez dans une étagère où les livres sont classés par ordre alphabétique des noms des auteurs, vous recherchez de lire le livre de Thomas H. Cormen puisque le nom commence par « T », lettre se trouvant à la 18^{ème} position dans l'alphabet, vous le cherchez aux environs des trois quart de l'étagère. La recherche dichotomique consiste à diviser en deux un tableau des éléments pour enfin examiner la valeur du milieu à la valeur recherchée. Supposons que la valeur du milieu ne correspond pas à la valeur recherchée, nous continuerons la recherche à gauche ou à droite du fait que le tableau est trié. En examinant une seule valeur nous avons éliminé la moitié des éléments du tableau qui ne nous intéresse pas. Nous continuons notre recherche au milieu de la moitié et examiner la valeur correspondante. Supposons encore que la nouvelle valeur du milieu ne correspond pas à la recherche, on continuera la recherche dans la moitié de la moitié. Ainsi de suite.

Imaginons si nous voulons rechercher x qui vaut 2 dans le tableau de 6 valeurs, nous ferons ce qui suit :

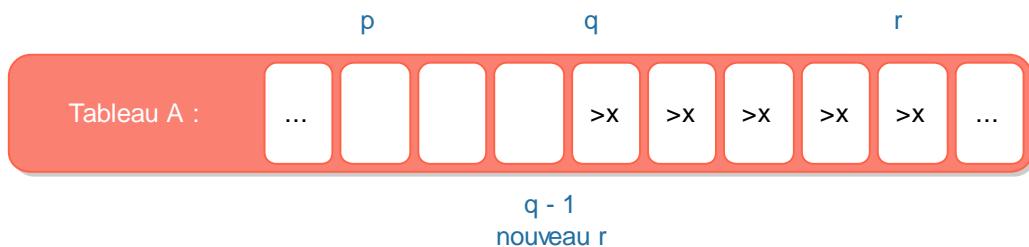


Dans un tableau, la recherche dichotomique examine la partie du tableau qui se trouve entre deux indices, ceux-ci inclus p et r . Initialement $p = 1$ et $r = n$. Supposons que nous recherchons la valeur x du tableau A . à chaque étape, nous examinons uniquement les sous-tableaux qui commence à $A[p]$ et se termine à $A[r]$ puisque nous allons manipuler les sous-tableaux, nous utilisons la notation $A[p \dots r]$. Nous déterminons le point central q du sous-tableau examiné en calculant la moyenne de p et de r , puis ignorons la partie fractionnaire si elle existe $q = (p + r) / 2$ nous utilisons la division entière. Nous vérifions si $A[q]$ est égal à x , dans l'affirmative nous avons terminé car nous pourrons simplement retourner q comme indice de l'emplacement où se trouve x dans le tableau A .

Si à la place, $A[q] \neq x$, alors nous exploitons l'hypothèse que le tableau A est trié. Puisque $A[q] \neq x$, nous avons deux possibilités :

- $A[q] > x$ c'est-à-dire x se trouve à gauche dans ce cas nous examinons les éléments de gauche
- $A[q] < x$ c'est-à-dire x se trouve à droite, dans ce cas nous examinons les éléments de droite.

Puisque le tableau est trié, nous savons non seulement que $A[q]$ est supérieur à x , mais également que, imaginant le tableau disposé de gauche à droite, chaque élément à droite de $A[q]$ est supérieur à x , par conséquent nous ne pouvons pas prendre en considération tous les éléments qui se trouvent à $A[q]$ et à sa droite. Pour l'étape suivante nous ne cherchons pas à p , mais r prend la valeur de $q - 1$.



Procédure Recherche-Dichotomique (A, n, x)

Entrées :

- A : un est tableau
- n : est le nombre d'élément de A
- x : est l'élément recherché

Début

p = 1

r = n

Tant que $p \leq r$ faire la chose suivante

$q = (p + r) / 2$

 Si $A[q] = x$ alors

 Retourne q

 Sinon

 Si $A[q] > x$ alors

$r = q - 1$

 Sinon

 Si $A[q] < x$ alors

$p = q + 1$

 Fin si

 Fin si

Fin Si

Fin tant que

Retourner -1

Fin

Exercice sur le mathématique de 8^e éducation base

1. Ecrire un algorithme et un programme python, qui lit un entier relatif au clavier et qui affiche sa valeur absolue.
2. Ecrire un algorithme et programme python qui lit un nombre décimal relatif au clavier qui calcule et affiche le carré de ce nombre ($carré = a^2$ avec $a \in \mathbb{Z}$).
3. Ecrire un algorithme et un programme python qui lit un nombre décimal relatif au clavier, qui calcule et affiche sa valeur cubique ($cube = a^3$ avec $a \in \mathbb{Z}$).

4. Ecrire un algorithme et un programme python qui lit au clavier deux nombres entiers relatifs, qui calcule et affiche respectivement leur somme et leur produit.
5. Ecrire un algorithme et un programme python qui lit un nombre inférieur ou égal 10 000 et l'écrit sous forme de puissance. Exemple 1 000, le programme doit afficher 1×10^3 .
6. Ecrire un algorithme et un programme python de résolution de cette expression a^n avec $n \in N$. Ce programme doit lire a et n au clavier.
7. Ecrire un algorithme et programme python de résolution de cette expression a^n avec $n < 0$. Ce programme doit lire a et n au clavier tout en vérifiant la valeur de n qui doit être inférieur à zéro.
8. Ecrire un algorithme et un programme python qui lit la désignation, le prix unitaire et la quantité d'un article vendu, qui calcule et affiche le prix total de cette façon.

Veuillez saisir la désignation du produit : *savon boom*

Quel est le prix unitaire de savon boom ? : 1000

Quelle est la quantité vendue ? : 5

Prix unitaire : 1000

Désignation : *savon boom*

Quantité : 5

Prix total : 5000 FC

9. Même que la question précédente, mais cette fois ce sont les informations de 3 articles qui seront saisies et l'affichage final ressemblera à ça :

| N° | Désignation | PU | Qt. | PT |
|----|----------------|-------|-----|-------|
| 1. | Pain crocodile | 1000 | 2 | 2000 |
| 2. | lait Nido | 20000 | 1 | 20000 |
| 3. | thé carioca | 5000 | 1 | 5000 |
| # | Total | | 4 | 27000 |

10. Ecrire un algorithme et un programme python qui lit un nombre décimal au clavier et l'affiche sous forme fractionnaire. Par exemple 2.5 donnera $25/10$.
11. Ecrire un algorithme et un programme python qui lit deux nombres entiers au clavier et qui affiche leurs diviseurs communs.
12. Ecrire un algorithme et programme python qui lit deux entiers au clavier, le numérateur et le dénominateur, qui le simplifie et affiche le résultat après simplification. Par exemple $\frac{3}{6} = \frac{3}{6} = \frac{1}{3}$ pour dire 3 et 6, le programme donnera 1 et 3.
13. Ecrire un algorithme et programme python qui lit le numérateur et le dénominateur d'une fraction et qui détermine si cette dernière est irréductible ou réductible.

14. Ecrire un algorithme et un programme python qui lit deux fractions de même dénominateur au clavier, qui calcule et affiche leur somme.
15. Ecrire un algorithme et un programme python qui lit deux fractions de dénominateurs différents au clavier, qui calcule et affiche leur somme.
16. Ecrire un algorithme et un programme python qui lit deux fractions de même dénominateur au clavier, qui calcule et affiche leur différence.
17. Ecrire un algorithme et un programme python qui lit deux fractions de dénominateurs différents au clavier, qui calcule et affiche leur différence.
18. Ecrire un algorithme et un programme python, qui affiche tous les diviseurs d'un entier saisi au clavier.
19. Ecrire un algorithme et un programme python qui lit deux entiers au clavier, qui calcule et affiche leur plus grand diviseur commun.
20. Ecrire un programme python qui affiche les multiples d'un entier saisi au clavier.
21. Ecrire un programme python qui calcule et affiche le plus petit commun multiple de deux entiers saisis au clavier.
22. Ecrire un programme python qui affiche le produit de deux fractions saisies au clavier.
23. Ecrire un programme python qui affiche le quotient de deux fractions saisies au clavier.
24. Ecrire un algorithme et un programme python, qui lit la quantité, le prix unitaire d'un article vendu, qui calcule et affiche la taxe sur la valeur ajoutée (TVA).
25. Ecrire un algorithme et un programme python, qui lit un nombre au clavier et qui détermine s'il est premier ou pas. (un nombre est premier, lorsqu'il n'a que deux diviseur : 1 et lui-même, exemple 11).
26. Ecrire un algorithme et un programme python, qui calcule et affiche la valeur numérique des expressions suivantes :
 - a. $2a + 13b + x - 5$
 - b. $3(a - b) - 3y$
 - c. $a + b^2 + y^2$
27. Ecrire un programme python qui lit au clavier une expression algébrique (un monôme) et qui détermine la partie littérale et la partie numérique. Par exemple($-5a^2b$). Qui s'écrire dans le programme comme suit $-5aE2b$, le programme doit afficher le résultat comme suit : -5 : numérique et aE2b littérale.
28. Ecrire un algorithme qui calcule et affiche l'aire d'un triangle.
29. Ecrire un programme python qui lit une expression mathématique au clavier et qui détermine si c'est monôme, binôme et trinôme.
30. Ecrire un programme python et un algorithme de résolution d'une équation du premier degré $ax + b = 0$ dans N et dans Z .
31. Ecrire un programme python et un algorithme de résolution d'une équation du second degré $ax^2 + xb + c = 0$.
32. Ecrire un algorithme et programme python, qui calcule et affiche l'aire d'un parallélépipède connaissant sa longueur, sa largeur et sa hauteur.

33. Ecrire un algorithme et un programme python qui calcule et affiche la surface d'un carré connaissant (son côté) la longueur d'un côté.
34. Ecrire un algorithme et un programme python, qui calcule le volume d'un cône.
35. Ecrire un algorithme et un programme python qui calcule le volume d'une sphère.
36. Ecrire un algorithme et programme python qui calcule et affiche volume d'un prisme.
37. Ecrire un algorithme et programme python, qui calcule et affiche le volume d'un cylindre.
38. Ecrire un algorithme et un programme python qui calcule et affiche l'air d'un cône.
39. Ecrire un programme python qui calcule et affiche la distance entre deux points dans un plan.
40. Ecrire un algorithme et programme python qui convertit en radian l'amplitude d'un angle donné en degré en en grade.
41. Ecrire un programme python qui calcule et affiche l'air d'un parallélogramme.
42. Ecrire un programme python, qui calcule et affiche la circonférence d'un cercle.
43. Ecrire un algorithme et programme python qui trie par ordre croissant dix entiers saisis au clavier.
44. Ecrire un programme python qui calcule la moyenne arithmétique des 10 entiers saisis au clavier.
45. Ecrire un programme python qui calcule la moyenne arithmétique pondérée des 10 entiers saisis au clavier.
46. Ecrire un programme python qui lit deux états de la matière et qui détermine l'état de passage entre les deux états saisis.

Bibliographie

Joel, Grus, Data science par la pratique, le fondamentaux avec python, Eyrolles, 2015.

Damien Séguy et Philippe Gamache, Sécurité PHP et MySQL, Eyrolles, 2007.

Thomas H. Cormen, Algorithme, notions de base, DUNOD, 2013.

Jean François PILLOU et Fabrice LEMAINQUE, Tout sur les réseaux, DUNOD, 2015.

Doug LOWE, les réseaux pour les nuls 10^e édition, les nuls, sd.

Yasmina Salmandjee et Paul Durand Desgranges, les réseaux sociaux pour les nuls, 2017.

Junior 0 et vinc 14, les réseaux pour les zéros, Openclassrooms, 2012.

Claude servin, réseaux et télécoms 4^e édition, DUNOD, 2013.

Rudi Brunchez, les bases de données NoSQL et le big data 2^e édition, Eyrolles.

Durlien VANNIEUWENHUIZE, l'intelligence artificielle vulgarisée, machine Learning et Deep Learning par la pratique, eni, sd.

Laurent Bloch et Christophe Wolfhugel, sécurité informatique, principe et méthode à l'usage des DSI, RSSI et administrateurs, Eyrolles, sd.