Chapitre 1 **Réseaux**

Introduction

- ***Discussion 1 : j'utilise le réseau social Instagram, comment fonctionne-t-il ?***

  Arriver (entre autres) à :
  - *Si j'utilise le réseau Instagram avec un ordinateur, il fonctionne au sein d'un réseau plus global appelé le web (la toile), plus précisément le world wide web (« www »).*
  - *Le web fonctionne grâce au support physique d'un réseau de communication entre machines informatiques : l'internet*
  - *Instagram, web et internet portent donc tous les trois le nom de réseau (discussions afin de commencer à établir des différences…)*
  - *…*
- ***Discussion 2, ouverte : qu'est-ce qu'un réseau ? Quelles précautions doit-on prendre pour qu'un réseau fonctionne ? (Que sous-entend le terme « un réseau fonctionne » ?)***

  Arriver (entre autres) à :
  - *L'information doit être intégralement transmise. La machine émettrice doit savoir que l'information envoyée est arrivée à destination.*
  - *L'information doit pouvoir circuler dans tous les sens.*
  - *Le chemin de transmission doit être optimisé.*
  - *…*
- ***Définitions (dictionnaire) du mot réseau :***
  - *Ensemble formé de lignes ou d'éléments qui communiquent ou s'entrecroisent.*
  - *Ensemble de routes, de voies navigables, de lignes aériennes ou de chemin de fer, qui relient différentes régions entre elles, qui appartiennent à une même compagnie.*
  - *Ensemble organisé dont les éléments, dépendant d'un centre, sont répartis en divers points : Le réseau des agences d'une banque. Réseau de distribution commerciale.*
  - *Ensemble de circuits, de canalisations et des appareils qui les relient, permettant la circulation et la distribution de l'électricité, de l'eau, du gaz, du téléphone, etc.*
  - *Etc.*

Et bien sûr :
  - *Ensemble d'ordinateurs connectés entre eux pour échanger des informations*

Il suffit de deux objets reliés, interconnectés pour considérer qu'un réseau est constitué.

- ***Avant de commencer : dans quel esprit abordons-nous ce contenu ?***

« IP », « TCP », « DHCP », « DNS », « HTML », « HTTP», « FTP », « LAN », « SMTP », « IMAP », « MAC », « WWW », … ETC !

Nous serons confrontés à de nombreux sigles et acronymes.
Il n'est pas question pour nous de détailler comment ils fonctionnent, mais plutôt de bien comprendre leur place et leur utilité dans le cadre du fonctionnement d'un réseau.

Exemple rapide :
http ://www.lyceecassinbayonne.fr l'adresse web d'un blog.
Les machines n'échangeant en réalité que des informations sous forme numérique (Puisque les machines informatiques ne gèrent que des 0 et des 1), l'adresse du site (du ou des serveur(s) qui héberge(nt) le site) est numérique.
Lorsque l'on fait la demande (« ***nslookup lyceecassinbayonne*** » en mode console ou invite de commande, voir pendant la séance), on nous propose plusieurs adresses :
2606 :4700 :3032:681c :92
104.28.1.146 etc. *(Les nombres présentés dans ces adresses sont en réalité codés en numération binaire)*

Nous ne chercherons pas à savoir comment le protocole DNS fonctionne, c'est-à-dire quelles sont les instructions réalisées par le programme permettant de convertir une adresse numérique (une adresse IP) en nom de domaine compréhensible.

Nous devons juste savoir que ce protocole existe et quelle est son utilité.

I - Réseaux informatiques, internet

1) Présentation

Un réseau Informatique relie physiquement entre elles des machines informatisées, des ordinateurs, des serveurs, etc.

L'informatique moderne est née dans les années 40 (Le mot « informatique » n'est apparu qu'à la fin des années 50).

Dès les années cinquante, les ordinateurs ont été mis en réseau afin d'échanger des informations, mais les premiers réseaux informatiques restaient très liés aux constructeurs d'ordinateurs ou aux opérateurs téléphoniques.

Les réseaux généraux, indépendants des constructeurs, sont nés aux États-Unis avec ArpaNet (1970) et en France avec Cyclades (1971).

Les efforts de développement d'un réseau planétaire indépendant ont alors été intenses et ont mené, en 1983, à internet.

Un réseau informatique peut bien entendu se déployer à petite échelle :

- Réseau Scribe du lycée Cassin : environ 350 ordinateurs, quelques dizaines d'imprimantes, des commutateurs (switches), un serveur, une passerelle.
- Réseau domestique privé : quelques ordinateurs, une passerelle (box internet), une imprimante, etc.

Intérêts d'un réseau informatique (***discussion***) :

- Partage de ressources
- Communication entre personnes (mail, chat, messageries diverses, réseaux sociaux, …)
- Communication entre procédés
- Unicité de la source d'information (base de données).
- Jeux multi-joueurs en ligne.

Il faut bien se rendre compte que tout cela n'existait pas il y a à peine 40 ans et considérer internet comme un progrès (***discussion***).

Nous insistons sur un point : Internet est le réseau dit « physique », c'est-à-dire le support qui permet la transmission de signaux contenant les informations à échanger. Dans la mesure où ce support physique existe, les informations peuvent y circuler indépendamment de celui-ci.

A titre de comparaison : les voies d'un réseau routiers permettent la circulation des véhicules. Si vous êtes empêché de circuler c'est très rarement parce que l'on a enlevé la route (cela peut arriver mais un autre chemin est proposé…).
Si la circulation est empêchée, c'est à cause d'interventions indépendantes de l'existence de la route (feux rouges, frontières, péages, interdictions diverses…)

Le réseau internet permet la transmission d'informations sous la forme de signaux.
Ces signaux sont essentiellement :

- Electriques
- Electromagnétiques (? : discussion en allumant éteignant la lumière afin de préciser l'emploi de vocabulaire adapté : lumière, transmission, signal, onde, onde électromagnétique, etc.)

2) Nature du lien physique entre les ordinateurs d'un réseau

a. Fil, cable

1ère solution : Les informations sont converties en impulsions électriques (La grandeur tension électrique, de symbole U, caractérise ces impulsions) et sont transmises sous forme de courant (La grandeur intensité du courant, de symbole I, caractérise ce courant)

Pour ce mode de transmission, nous avons donc besoin d'un support conducteur : un fil ou un câble métallique. Nous rappelons que l'entité qui circule est ici l'électron. Il y a donc déplacement de matière pour transférer de l'information (un peu comme lorsque le facteur porte une lettre…)

Exemples :
- Câble éthernet (ou RJ45)
- Câbles sous-marins transatlantiques

Dans la presse (été 2020) :
« Google a annoncé, mardi 28 juillet, qu'il allait déployer un nouveau câble transatlantique consacré au transit des données Internet. Avec une date de mise en service prévue pour le courant 2022, cette nouvelle infrastructure – nommé Grace Hopper, en hommage à l'informaticienne américaine (1906-1992) – doit relier New York à Bude (Royaume-Uni) et Bilbao (Espagne).
Une fois fonctionnel, il permettra à Alphabet, la maison mère de Google, de posséder à elle seule deux des 19 câbles transatlantiques reliant actuellement l'Amérique du Nord à l'Europe occidentale. Avec ces câbles, Alphabet sera ainsi capable d'assurer la connexion de ses plates-formes de contenus (YouTube, Gmail, Google Docs…) entre les deux continents en toute autonomie… » (Le Monde août 2020)

Exposé sur la nature, la constitution des câbles transatlantiques.

2ème solution : Lorsque nous communiquons par l'intermédiaire de notre smartphone, c'est différent : nous sommes dans les domaines du wifi, du bluetooth et des réseaux mobiles 3G, 4G, 5G.

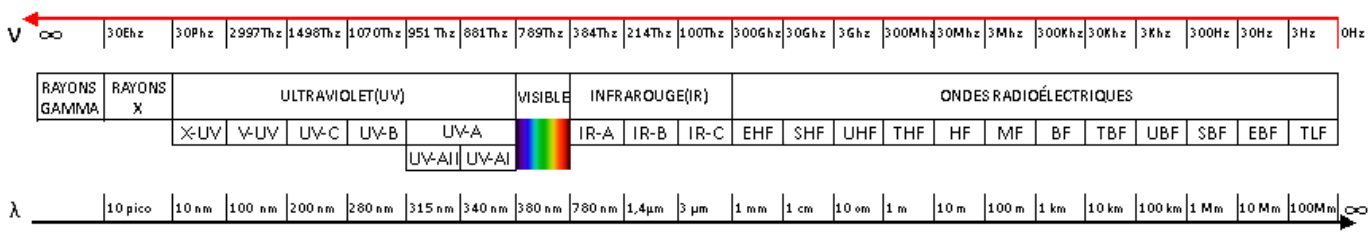
L'information, toujours initialement convertie en signal électrique, est ensuite convertie (par l'intermédiaire d'une antenne) en onde électromagnétique qui se propage et se transmet. A la réception, le processus inverse est à l'œuvre : conversion en signal électrique à l'aide d'une antenne (réceptrice).

L'onde ne transporte aucune matière, mais l'information est toutefois transmise (comme lorsque vous entendez quelqu'un qui vous appelle : un onde sonore s'est propagé jusqu'à vos oreilles)

Les ondes servant de support à la transmission d'informations dans le domaine de l'informatique sont des ondes électromagnétiques. La lumière est une des catégories d'ondes électromagnétiques.

Dans le vide, toute les ondes E.M. se propagent à la même vitesse (on dit plutôt célérité…*Discussion*), notée c, de valeur 300000 km/s.
Ce qui différenciera deux ondes E.M. sera une autre grandeur : la fréquence.

Nous n'allons pas expliquer aujourd'hui ce que représente cette grandeur, mais elle nous intéresse car elle permet de délimiter certains domaines :



THÉORIE, DOMAINES DU SPECTRE ÉLECTROMAGNÉTIQUE

Bluetooth : 2,4 GHz, portée de quelques mètres
Wi-Fi 2,45 GHz (partagé avec le bluetooth) et 5 GHz, portée de quelques dizaines de mètres
3G : 1900 et 2100 MHz, débit quelques centaines de kbits/s (jusqu'à quelques Mbits/s)
4G : 800, 1600 et 2600 MHz (entre autres), débit pouvant théoriquement aller jusqu'à 150 Mbits/s, mais en réalité on peut compter sur des échanges d'informations 3 fois plus rapides qu'avec la 3G.
5G : 1452-1492 MHz, débit prévu pour le transfert d'informations : 10 Gbits/s
La portée d'une antenne émettrice 4G peut varier de moins d'1 km à environ 30 km (cela dépend de l'environnement géographique).

Nous voilà (presque) rassurés, les bandes de fréquences utilisées par les réseaux de transmissions numériques appartiennent toutes aux domaines des ondes infrarouge ou des ondes radio, réputées sans danger…

3ème solution : nous transmettons à l'aide d'ondes E.M., mais nous guidons ces ondes dans un conduit, c'est la transmission par fibre.

Discussion : Avantages et inconvénients

- Energie dissipée
- Dispersion
- Coût
- Débits (voir plus haut)

3) Fonctionnement : questions

Question 1: Le réseau local du lycée est constitué d'environ 350 ordinateurs. Comment procéder pour qu'un envoi d'informations depuis un ordinateur A arrive uniquement à un ordinateur B sans qu'il y ait interaction avec tous les autres ordinateurs du réseau ?

Question 2 : La même que la question 1, mais l'ordinateur destinataire appartient à un autre réseau local, par exemple celui du lycée Cantau.

Pistes pour la réponse :
- Chaque ordinateur doit être défini, caractérisé par un nom, un code d'identification.
- A l'information envoyée doit être associé une description du chemin à prendre et, bien entendu, « l'adresse » des ordinateurs A et B.
    - Et s'il y a plusieurs chemins (routes) possibles ?
        - Y en a-t-il de meilleurs que d'autres ou bien est-ce juste pour palier à d'éventuelles pannes ?

Nous pourrions nous lancer dans l'activité « routage débranché » p 39 du livre, mais nous ne pouvons pas envisager cette activité tant que nous n'avons pas clairement différencié différents types de machines, en particulier les simples ordinateurs et les routeurs.

Question 3 : une information « volumineuse » (un ensemble de fichiers, une vidéo, un ensemble d'instructions destinées à faire fonctionner un procédé dans une usine, etc.) est transmise par internet. Au cours de la transmission, une courte panne de réseau se produit. Comment l'information peut-elle toutefois arriver intacte à destination ? Et s'il s'agit d'une information pour laquelle nous n'avons aucune prise sur son caractère temporel, par exemple une visioconférence en direct ?

Pistes de réponses :
- Trouver un autre chemin à travers le réseau afin de ne pas interrompre la transmission, cela s'appelle le routage, auquel sont évidemment associé des algorithmes et des programmes.
- Envoyer l'information par morceaux (nous dirons par paquets) avec un protocole de validation de l'arrivée de chaque paquet.
- Activité élèves : tout sera regroupé au cours d'une activité de reconstitution d'un réseau à l'aide du logiciel de simulation Filius.

4) Le protocole TCP / IP va répondre à toutes nos questions

a. Qu'est-ce qu'un protocole réseau ?

Un protocole est une méthode standard (*) qui permet la communication entre des processus, c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

b. Que doit gérer ce protocole ?

Nous nous intéressons aux protocoles orientés connexion : ce type ce protocole contrôle la transmission des données pendant la communication entre deux machines.

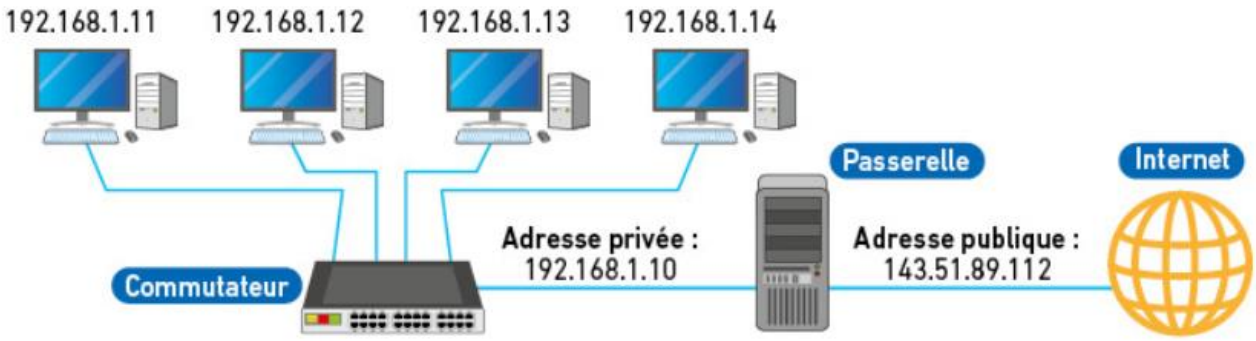
Il est donc évident que chaque machine doit être identifiée, par une adresse (comme l'adresse d'un domicile), à la fois pour que la machine émettrice connaisse l'adresse de la machine destinataire et pour que la machine destinataire puisse renvoyer une confirmation de réception.

c. Le protocole IP (« Internet Protocol »), l'adresse IP d'une machine

De nature logicielle, internet s'appuie sur une grande variété de réseaux physiques où IP est implémenté. Il uniformise l'accès à tous les ordinateurs, les téléphones et les objets connectés. Le protocole IP gère donc les adresses ainsi que le routage.

Chaque machine reliée directement à l'internet public se voit attribuer une adresse dite adresse IP. Dans l'idéal, chaque ordinateur connecté au réseau public doit posséder une adresse IP unique.

Attention, si votre ordinateur est relié à un serveur ou à une passerelle, il n'est plus connecté directement au réseau public, c'est le l'ensemble {commutateur + passerelle} qui assure cette connexion. L'adresse de votre ordinateur n'est pas une adresse unique au niveau mondial. Son adresse IP existe, mais elle est locale.
Votre machine n'est donc pas accessible directement depuis le réseau internet public.
Nous reprenons ici la figure se trouvant au bas de la page 38 du manuel :



Le protocole IP actuel le plus courant est le protocole IPv4 (il tend à être remplacé par IPv6)

L'adresse IP se présente sous la forme de 4 nombres entiers (écrit en numération décimale) séparés par des points. Chacun des 4 nombres peut prendre une valeur entre 0 et 255.

Exemple : 194.153.205.26

Sur la figure ci-dessus, les adresses commençant par 192 sont des adresses privées. Il est donc possible que dans d'autres réseaux locaux on retrouve ces mêmes adresses attribuées à d'autres machines.

Trouver l'adresse IP de l'ordinateur sur lequel vous travaillez : activité n°6 p 38 du manuel de SNT.
Dans la barre de recherche Windows, tapez « cmd » et sélectionner la proposition « cmd.exe ». Dans la fenêtre qui s'ouvre vous pouvez entrer différentes instructions vous permettant de collecter des informations.
Suivre les instructions de l'activité 8 p 40 (« ipconfig » puis « ping qwant.fr »)

Comparez vos résultats avec ceux des groupes voisins, commentez les différences entre l'adresse IP de votre poste et l'adresse IP du serveur.

Revenir au cours suivant avec l'adresse IP de l'ordinateur de votre domicile, celle de tous les périphériques associés et celle de votre box.
(Mêmes instructions que dans l'exercice précédent, ici l'adresse du serveur est celle du serveur auprès duquel vous avez souscrit un abonnement (orange, free, etc.))

A titre d'exemple le résultat obtenu sur mon ordinateur personnel utilisé à mon domicile :

```
PS C:\Users\jean-> ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . . :

Carte réseau sans fil Connexion au réseau local* 1 :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . . :

Carte réseau sans fil Connexion au réseau local* 2 :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . . :

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . . : home
   Adresse IPv6 de liaison locale. . . . . .: fe80::6073:262e:b527:484c%7
   Adresse IPv4. . . . . . . . . . . . . . .: 192.168.1.54
   Masque de sous-réseau. . . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . . : 192.168.1.1

Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . . :
PS C:\Users\jean-> ping qwant.fr

Envoi d'une requête 'ping' sur qwant.fr [217.70.184.55] avec 32 octets de données :
Réponse de 217.70.184.55 : octets=32 temps=38 ms TTL=54
Réponse de 217.70.184.55 : octets=32 temps=40 ms TTL=54
Réponse de 217.70.184.55 : octets=32 temps=39 ms TTL=54
Réponse de 217.70.184.55 : octets=32 temps=44 ms TTL=54

Statistiques Ping pour 217.70.184.55:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 38ms, Maximum = 44ms, Moyenne = 40ms
PS C:\Users\jean->
```

Si je me connecte (même ordinateur) par l'intermédiaire de mon smartphone en passant par le réseau 4G :

```
PS C:\Users\jean-> ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 1 :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Connexion au réseau local* 2 :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::6073:262e:b527:484c%7
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.43.218
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.43.241

Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :
PS C:\Users\jean-> ping qwant.fr

Envoi d'une requête 'ping' sur qwant.fr [217.70.184.55] avec 32 octets de données :
Réponse de 217.70.184.55 : octets=32 temps=46 ms TTL=48
Réponse de 217.70.184.55 : octets=32 temps=70 ms TTL=48
Réponse de 217.70.184.55 : octets=32 temps=56 ms TTL=48
Réponse de 217.70.184.55 : octets=32 temps=42 ms TTL=48
```

Si je me connecte (même ordinateur) sur le réseau du lycée :

Nous pouvons aussi utiliser IP2, un logiciel très simple d'utilisation qui permet d'obtenir les adresses IP souhaitées (locale et publique).

A propos des adresses IPv4, une dernière question :

Pourquoi des nombres entre 0 et 255 ? Combien d'adresses IPv4 existent en tout ?

Un groupe volontaire pour un exposé rapide sur IPv6 ?
Un groupe volontaire pour un exposé sur les masques de sous-réseau ?

Une analogie claire peut être établie entre un numéro de téléphone fixe et une adresse IP, il y a de réelles similitudes de conception.

d. Que représentent les différentes parties d'une adresse IPV4 ?

Nous nous contentons ici d'une approche très simplifiée et résumée, mais il est important de comprendre l'essentiel :

- Partant de la gauche de l'adresse IPv4, nous trouvons d'abord les octets désignant l'adresse du réseau (netID) puis ceux désignant les adresses des machines connectées sur ce réseau (hostID).
    - Si le réseau contient peu de machines, on n'a besoin que du dernier octet (le plus à droite) pour les désigner et les trois premiers octets donnent l'adresse du réseau.
    - Si le réseau est constitué d'énormément de machines, il peut être nécessaire d'utiliser les deux, voire les trois octets de droite de l'adresse IPv4. Cela ne laisserait qu'un octet de l'adresse (celui de gauche)

pour indiquer le réseau. Cette situation concerne donc les réseaux très importants qui ne sont obligatoirement peu nombreux.

- Le masque de sous-réseau permet en fait de savoir comment sont répartis les octets dans les adresses des machines d'un même réseau. Dans mon réseau domestique, La masque, qui est aussi un code type IPv4, est du type 255.255.255.000, soit, en langage binaire :
  11111111.11111111.11111111.00000000
  Ce code couplé à l'adresse d'une machine du réseau codera un 0 pour tout bit de l'adresse de la machine de même rang qu'un 0 dans le masque de sous réseau et codera un bit inchangé pour les bits de même rang que des 1 dans le masque.
  Exemple :
  L'adresse 10110011.10111111.00001111.00001111 confrontée au masque :
  11111111.00000000.00000000.00000000 donnera le résultat :

  10110011.00000000.00000000.00000000
  (179.0.0.0 en présentation décimale)

  On ne voit plus que l'adresse du réseau sans voir l'adresse complète d'une machine de ce réseau.

- Une adresse qui se termine par un, deux ou trois 0 est obligatoirement l'adresse d'un réseau (aucune machine, ordinateur ou autre périphérique ne possède une adresse contenant des 0 dans les différents octets de cette adresse. Les zéros sont réservés, par exemple, à la passerelle qui relie les machines d'un sous réseau au réseau internet

Exposés : adresses IP de classes A, B, C. Adresses IP réservées.

e. L'adresse symbolique, le protocole DNS

Activité 9 p 40 / Activité Filius (voir séance ultérieure)

f. Le routage

Activité 10 p 40 et activité débranchée 7 p 39

En mode invite de commande : « tracert *adresse de votre choix* »
Il ne faut pas hésiter à renouveler exactement la même demande afin de comprendre que la connexion ne sefera pas forcément toujours par le même chemin.

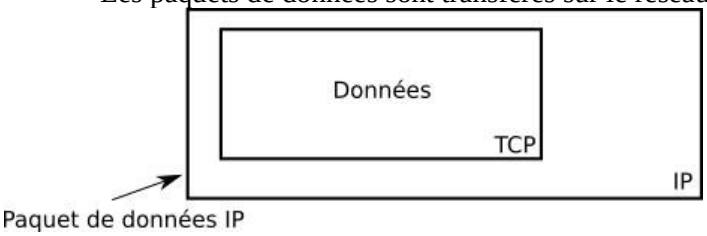
g. Le chemin d'un mail selon le protocole IP

Voir activité Internet Filius (voir séance ultérieure)

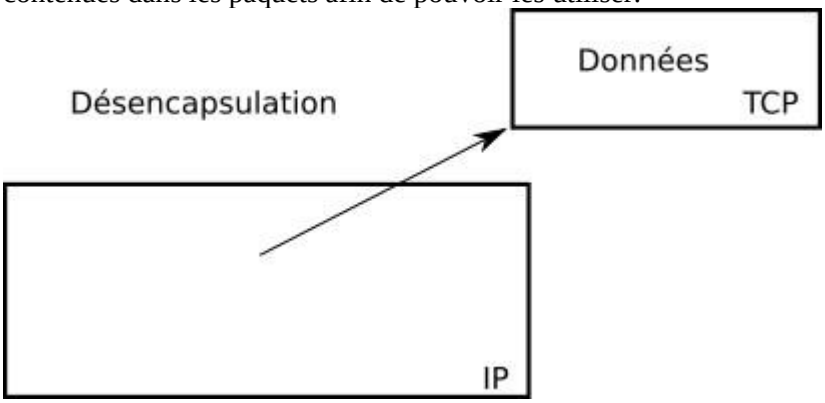
h. l'envoi de données plus volumineuses: le protocole TCP (« transmission control protocol », protocole de contrôle de la transmission) / IP (« internet protocol »)

Considérons un envoi de données d'un ordinateur A vers un ordinateur B.

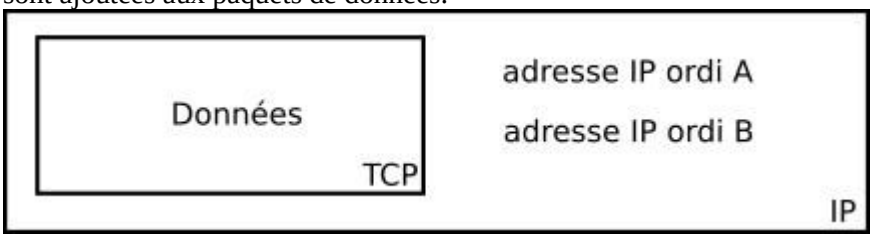
- A utilise d'abord le protocole TCP pour mettre en forme les données à envoyer.
- Le protocole IP utilise les données mises en forme par le protocole TCP afin de créer des **paquets de données**. On dit que le protocole IP **encapsule** les données issues du protocole TCP (voir l'annexe « encapsulation des données »)
- Les paquets de données sont transférés sur le réseau de A jusqu'à B.



Une fois arrivées à destination (ordinateur B), les données sont "désencapsulées" : on récupère les données TCP contenues dans les paquets afin de pouvoir les utiliser.

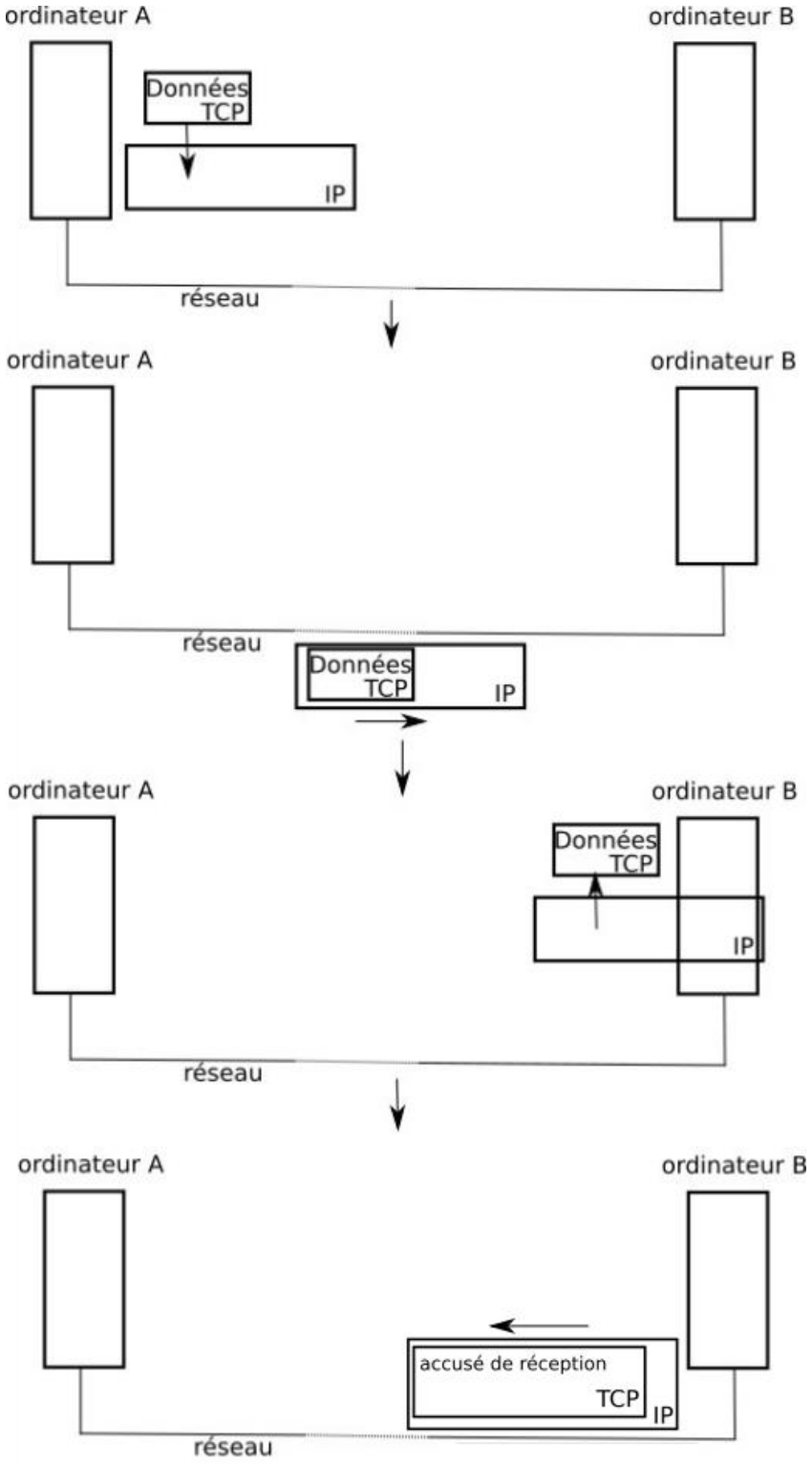


Le protocole IP s'occupe uniquement de faire arriver à destination les paquets en utilisant l'adresse IP de l'ordinateur de destination. Les adresses IP de l'ordinateur de départ (ordinateur A) et de l'ordinateur destination (ordinateur B) sont ajoutées aux paquets de données.



Le protocole TCP permet de s'assurer qu'un paquet est bien arrivé à destination. En effet quand l'ordinateur B reçoit un paquet de données en provenance de l'ordinateur A, l'ordinateur B envoie un accusé de réception à l'ordinateur A (un peu dans le genre "OK, j'ai bien reçu le paquet"). Si l'ordinateur A ne reçoit pas cet accusé de réception en provenance de B, après un temps prédéfini, l'ordinateur A renverra le paquet de données vers l'ordinateur B.
TCP/IP repose sur la notion de paquets de données transférés d'une machine à une autre. Une donnée volumineuse va donc être découpées en plusieurs morceaux, chacun d'entre eux étant envoyé dans un paquet différent.
C'est au cours du transfert proprement dit qu'intervient le protocole de routage qui va être abordé dans la partie suivante. Nous comprenons donc que chaque paquet ne prend pas forcément la même route, d'où l'importance du protocole d'accusé de réception renvoyé de B vers A.
La donnée globale ne pourra être reconstituée que si tous les paquets ont été transférés de A vers B.
Ce n'est qu'une fois tous les paquets arrivés à destination que le fichier d'origine pourra être reconstitué.

Résumé :



5) ***Deux catégories de communications sur internet***
   - ***a.*** Client/serveur
   - ***b.*** Peer to peer **Voir activité Internet Filius**

6) ***Regard critique***

Annexes pour la partie I

Copie de l'exercice de la page 38 du manuel

En salle informatique, les ordinateurs ont habituellement des adresses spécifiques liées au réseau local auquel ils sont connectés.

1. a. Rechercher les paramètres de la connexion réseau de l'ordinateur.
b. Noter l'adresse IP.

2. Comparer les adresses obtenues sur plusieurs ordinateurs.

3. Vérifier si cette adresse est de la forme 192.168.x.y ou 10.*x.y.z* ou encore 172.*x.y.z* avec *x* compris entre 16 et 31.
Si oui, il s'agit d'une adresse locale à ce réseau.

4. Pour confirmer qu'une adresse est privée, se connecter via internet à un site révélant l'adresse IP des machines qui s'y connectent. C'est une adresse publique qui y est révélée : identique pour toute les machines du réseau privé.
Noter cette adresse : elle doit être différente de celle obtenue en question 1.

Le mode console ou invite de commandes

Le système ouvre une fenêtre qui permet de gérer des échanges d'informations entre l'ordinateur et l'extérieur, ce qui ne semble pas spécialement original.
Ce mode de fonctionnement permet toutefois d'accéder rapidement à certaines informations.
Les instructions sont souvent très basiques et consistent la plupart du temps en une demande d'information. La réponse se présente sous la forme d'une succession de lignes de valeurs, de codes, ou de phrases simples.

L'interface de la fenêtre console n'est pas graphique et la syntaxe des instructions et réponses est propre à ce mode de fonctionnement.
Il peut être très utile, mais demande la maitrise d'un langage supplémentaire ou, du moins, la connaissance d'un ensemble d'instructions spécifiques.
Sous certains systèmes, en particulier le système Linux, le mode console est couramment utilisé.

Ci-dessous quelques exemples de commandes (catégorie gestion des connexions réseau) :

- ***CONTROL NETCONNECTIONS*** *ou* ***NCPA.CPL*** *: ouvre les connexions réseau.*
- ***FIREWALL.CPL*** *: ouvre le pare-feu Windows.*
- ***IPCONFIG*** *: affiche les configurations des adresses IP de l'ordinateur.*
- ***WF.MSC*** *: ouvre les fonctions avancées du pare-feu Windows.*

Microsoft met à disposition une abondante documentation sur les commandes. A titre d'exemple, le lien permettant d'acéder à la page de description de la commande « ping » :
https://docs.microsoft.com/fr-fr/windows-server/administration/windows-commands/ping

L'encapsulation des données

II Utilisation du réseau internet pour constituer un réseau numérique : le web

- Présentation
- Les langages du web : html et css
    - Le décryptage d'une page web
    - La réalisation d'un site
-

III Un réseau au sein du www : le réseau social

WhatsApp, Twitter, Facebook, Snapchat : qui chiffre les messages privés des utilisateurs ?

Le chiffrement de bout en bout peut protéger d'un piratage de grande ampleur, comme celui qu'a subi récemment Twitter, mais n'est pas mis en place partout.

Des pirates sont accusés d'avoir manipulé des employés de Twitter pour obtenir l'accès à des outils internes du réseau social. Matt Rourke / AP

Deux semaines après que des comptes Twitter de personnalités de premier plan ont été utilisés frauduleusement pour diffuser des arnaques liées au bitcoin (une monnaie virtuelle), les conséquences pourraient être de long terme pour le réseau social.

Selon les sources de Bloomberg, les pirates à l'origine de cette fraude ont piégé au moins un employé de Twitter pour obtenir l'accès à un outil interne à l'entreprise. Selon l'enquête interne du réseau social, les messages privés de nombreux comptes ont également été consultés par les hackeurs.

Ce scandale remet sur le devant de la scène une problématique récurrente : sur certains services, les messages dits « privés » ne le sont pas vraiment, et peuvent être stockés sur les serveurs d'un réseau social, voire consultables par des employés de ces entreprises. Comment empêcher cela d'arriver ?

Lire aussi La version gratuite de Zoom ne bénéficiera pas du chiffrement des communications

Certains services chiffrent les échangent, d'autres non

Certains réseaux sociaux ou messageries chiffrent de bout en bout les échanges privés entre utilisateurs. Le chiffrement de bout en bout d'une conversation entre deux personnes signifie que seuls l'émetteur et le destinataire peuvent lire un message envoyé. Le message est transformé à l'aide d'un algorithme et d'une clé de chiffrement, et est déchiffré par le destinataire, qui détient une clé de déchiffrement du message. Ainsi, si une personne extérieure intercepte la conversation, elle n'a accès qu'à une suite complexe de caractères presque impossibles à décrypter sans clé. En théorie, une entreprise qui propose une messagerie chiffrée de bout en bout ne possède pas elle-même les clés pour déchiffrer les messages, seuls les utilisateurs concernés les ont.

Pourquoi il s'agit d'une question sensible

Si les échanges entre utilisateurs ne sont pas chiffrés de bout en bout, cela signifie qu'ils sont potentiellement stockés et lisibles par l'entreprise. Les réseaux sociaux disposent généralement d'outils en interne pour la modération des contenus et des utilisateurs, ou pour traiter les demandes formulées par les autorités dans le cadre d'enquêtes judiciaires.

Selon Bloomberg, environ 1 500 employés de Twitter ont des droits d'accès à certaines informations personnelles ou peuvent agir sur les comptes des utilisateurs (adresse IP, réinitialisation du mot de passe, etc.). Le média ne précise pas combien ont accès ou peuvent demander l'accès aux messages privés d'utilisateurs.

Mais alors, quelles plates-formes utilisées quotidiennement par les internautes procèdent au chiffrement ?

- ## *Twitter : non*

Twitter n'a jamais chiffré les échanges privés entre utilisateurs. C'est un sujet sur lequel l'entreprise est très régulièrement interpellée par les organisations de défense de la vie privée. Récemment, l'Electronic Frontier Foundation, une ONG internationale qui défend les libertés individuelles et la vie privée, a renouvelé son appel à Twitter, lui demandant de changer ses pratiques sur le sujet.

« Twitter n'aurait pas à s'inquiéter du fait que les intrus de ces dernières semaines aient lu ou exfiltré des messages privés si ces derniers avaient été chiffrés de bout en bout depuis le début, comme nous le demandons à l'entreprise depuis des années. »

En novembre 2019, deux employés de Twitter ont été arrêtés par la justice américaine, ils étaient soupçonnés d'avoir recueilli en interne des informations confidentielles sur certains utilisateurs du réseau social pour le compte du gouvernement saoudien.

- ## *Facebook Messenger : oui et non*

Par défaut, les conversations dans Facebook Messenger ne sont pas chiffrées de bout en bout. Le PDG de Facebook, Mark Zuckerberg, a fait la promesse de changer cet état de fait en mars 2019.
Aujourd'hui, les utilisateurs de Facebook ont la possibilité de créer des « conversations secrètes », qui sont chiffrées de bout en bout, mais ce chiffrement ne s'applique pas aux anciennes conversations, et il n'est pas possible de se mettre à protéger des conversations déjà en cours (si vous avez une longue conversation de groupe avec des amis par exemple).
Jon Millican, ingénieur pour Facebook Messenger, avait expliqué en janvier dernier à Wired qu'il ne fallait pas s'attendre à voir arriver un chiffrement par défaut de 100 % des conversations avant « plusieurs années ».

- ***Instagram : non***

Bien que Facebook ait évoqué l'intention d'unifier ses services de messagerie entre WhatsApp, Instagram Direct et Facebook Messenger, aucune conversation privée entre utilisateurs d'Instagram n'est chiffrée de bout en bout à ce jour.

- ***WhatsApp : oui***

Facebook, qui détient l'appli, assure que les messages envoyés d'un compte WhatsApp à un autre sont chiffrés de bout en bout, en s'appuyant sur un protocole éprouvé et reconnu par la communauté des spécialistes en sécurité informatique. Mark Zuckerberg a lui-même assuré qu'il était impossible pour Facebook de lire les messages échangés entre deux utilisateurs de WhatsApp. Mark Zuckerberg, s'exprimant devant le Sénat américain, l'a confirmé en 2018 :
« Nous ne lisons aucun contenu dans WhatsApp, tout est chiffré. »
Il est à noter que le chiffrement de bout en bout par défaut est également appliqué par Apple pour les messages envoyés d'un iPhone à l'autre sur iMessage, ainsi que par l'application Signal, disponible sur Android et iOS.

- ***Snapchat : oui et non***

Les messages écrits envoyés entre deux utilisateurs de Snapchat ne sont pas chiffrés de bout en bout, et sont stockés, selon Snapchat, pendant trente jours sur les serveurs de l'entreprise. Le réseau social a annoncé en janvier 2019 que les « Snaps » (photos et vidéos) envoyés entre deux utilisateurs sont, eux, bien chiffrés, et qu'ils sont supprimés des serveurs dès l'ouverture par le destinataire, ou de vingt-quatre heures à trente jours après l'envoi s'ils ne sont pas ouverts.
En mai 2019, une enquête du site Vice a révélé que des employés de Snapchat avaient utilisé frauduleusement un outil interne pour accéder aux informations confidentielles d'utilisateurs.

- ***TikTok : non***

L'application propose à ses utilisateurs une messagerie privée, mais explique sur son site que le contenu de ces messages est automatiquement collecté et lisible par l'entreprise et peut-être communiqué aux autorités dans le cadre d'une enquête judiciaire.

- ***Tinder : non***

Les conversations entre utilisateurs de Tinder, l'une des plus importantes applications de rencontres, ne sont pas chiffrées de bout en bout.

- ***Discord : non***

Discord est un outil, notamment privilégié dans les communautés liées aux jeux vidéo, qui permet aux utilisateurs de créer des groupes de discussion, composés de plusieurs espaces d'échange, aussi bien à l'écrit qu'à l'oral et en vidéo. Il est également possible d'échanger des messages privés entre deux utilisateurs, ou d'appeler un autre internaute.
A notre connaissance, aucun message, écrit, audio ou vidéo, n'est chiffré de bout en bout sur Discord.

- ***Slack : non***

Ce service de messagerie est commercialisé auprès des entreprises, et ne propose pas de chiffrement de bout en tout des discussions entre deux utilisateurs.
Le service de messagerie de groupe propose à certains de ses clients un système nommé Enterprise Key Management, qui permet à chaque entreprise de gérer ses propres clés de chiffrement pour protéger les messages et données qui la concernent et qu'elle stocke. Mais le fait que les conversations ne soient pas chiffrées de bout en bout signifie qu'en principe, soit le gestionnaire du Slack de votre entreprise, soit Slack lui-même peut avoir accès aux messages que vous envoyez.

- ***Skype : oui et non***

Le service de messagerie écrite, audio et vidéo a lancé en 2018 la possibilité pour les utilisateurs de créer des conversations écrites et audio chiffrées de bout en bout, sans que Skype lui-même ne puisse en obtenir le contenu. Mais cette option, qui ne concerne pas les appels vidéo, n'est pas activée par défaut.
(Le Monde août 2020)

Analogie finale :

Internet serait le réseau ferroviaire…
Le web serait les trains qui y circulent…
Les réseaux sociaux seraient les personnes qui circulent dans un train et passent d'un wagon à l'autre…