COURS DE SNT (Sciences numériques et technologie)

Classe : Seconde *Thème 1* *Mr BANANKO K.*	LYCÉE INTERNATIONNAL COURS LUMIÈRE **INTERNET** Chap 1

OBJECTIFS DU COURS

- *Distinguer le rôle des protocoles IP et TCP.*
- *Caractériser les principes du routage et ses limites.*
- *Distinguer la fiabilité de transmission et l'absence de garantie temporelle.*
- *Sur des exemples réels, retrouver une adresse IP à partir d'une adresse symbolique et inversement.*
- *Décrire l'intérêt des réseaux pair-à-pair ainsi que les usages illicites qu'on peut en faire.*
- *Caractériser quelques types de réseaux physiques : obsolètes ou actuels, rapides ou lents, filaires ou non.*
- *Caractériser l'ordre de grandeur du trafic de données sur internet et son évolution.*

I- Introduction

Que se passe-t-il lorsque vous tapez dans la barre d'adresse de votre navigateur **«http://www.google.fr»** ?

Votre ordinateur va chercher à entrer en communication avec un autre ordinateur se trouvant probablement à des milliers de kilomètres de chez vous. Pour pouvoir établir cette communication, il faut bien sûr que les 2 ordinateurs soient « reliés ». On dira que nos 2 ordinateurs sont en réseau. Il existe énormément de réseaux (la plupart des ordinateurs du lycée sont en « réseau »), certains réseaux sont reliés à d'autres réseaux qui sont eux-mêmes reliés à d'autres réseaux... ce qui forme « des réseaux de réseaux de réseaux...». Savez-vous comment on appelle cet assemblage multiple de réseaux ? **Internet !**

L'idée de relier des réseaux d'ordinateurs à d'autres réseaux d'ordinateurs date du début des années 70 avec le projet ARPAnet « *Advanced Research Projects Agency NETwork* » (Réseau reliant plusieurs universités des Etats-Unis) qui est, avec juste raison, considéré comme l'ancêtre d'internet.

Voici une vidéo qui va vous permettre de comprendre les principes de base d'internet. Nous aurons au cours de l'année l'occasion de reprendre les concepts abordés dans cette vidéo d'introduction en rentrant un peu dans les détails.

Activité 1.1

Après avoir visionné cette vidéo, faites-en un résumé de quelques lignes.

Solution

Comme expliqué dans la vidéo ci-dessus, afin de pouvoir s'identifier, tout ordinateur possède une adresse sur un réseau : son adresse IP.

Une adresse IP est de la forme "74.125.133.94" (cette adresse IP correspond au serveur de google "google.fr")

Les adresses IP sont de la forme : "a.b.c.d", avec a, b, c et d des nombres compris entre 0 et 255. Nous aurons l'occasion de revenir là-dessus un peu plus tard.

N.B. Une autre norme est en train d'être déployée, la norme IPV6 (alors que les adresses IP vues ci-dessus appartiennent à la norme IPV4). Pourquoi cette nouvelle norme ? Parce qu'avec le système IPV4, il risque, dans les prochaines années, de manquer d'adresses IP disponibles sur internet.

II- Repère Historique

ACTIVITÉ 1

Repères historiques

1961

Naissance de la communication par paquets

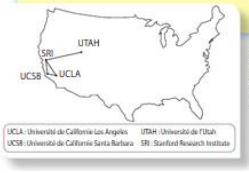
Dans les années 1950, l'US Air Force (armée de l'air américaine) cherche un moyen de communiquer, même en cas d'attaque nucléaire. L'Américain Paul Baran et le Britannique Donald Davies effectuent des recherches qui aboutissent en 1961. Leur solution est de découper les messages en **paquets** pouvant circuler à travers les multiples chemins d'un **réseau**. Ainsi, si un chemin est coupé, le paquet peut en prendre un autre et arriver à son destinataire.

Donald Davies est l'un des concepteurs de la notion de paquets.

1969

Les premiers réseaux d'ordinateurs

Les premiers réseaux d'ordinateurs datent de la fin des années 1950 comme le système de radar semi-automatique américain SAGE. En 1969, sous l'impulsion de l'informaticien américain Joseph Licklider, naît le réseau **Arpanet**. Pour la première fois, les données, découpées en paquets, transitent grâce à un **protocole de communication**, c'est-à-dire un ensemble de règles qui régissent les échanges. Paquet et protocole sont à la base d'**Internet** ce qui fait d'Arpanet son ancêtre.



En 1969, Arpanet connecte quatre réseaux d'ordinateurs dans des universités américaines.

1974

Naissance du protocole TCP

Vinton Cerf (à gauche) et Robert Kahn (à droite) récompensés en 2005 par le président George Bush pour avoir aidé à la création d'Internet.

Depuis Arpanet, les réseaux deviennent de plus en plus étendus ce qui nécessite des règles de communication plus élaborées. En 1974, les Américains Robert Kahn et Vinton Cerf inventent le protocole de communication *Transmission Control Program* qui s'occupe à la fois de la gestion des paquets (par exemple leur numérotation) et de la route qu'ils doivent suivre dans le réseau pour arriver à destination. Par la suite, ce protocole est scindé en deux, l'un gérant spécifiquement les paquets *(Transmission Control Protocol)* et l'autre les conduisant dans le réseau *(Internet Protocol)*, et devient le **TCP/IP**.

1989

Démocratisation d'Internet

Jusqu'à la fin des années 1980, Internet est un outil qui demeure très technique pour le grand public. Accéder à un ordinateur distant, y lire ou y déposer des données ne se fait pas encore en quelques clics de souris. Tout cela change avec l'arrivée du **Web** inventé par le Britannique Tim Berners-Lee. Internet et le Web sont donc deux choses différentes ! Internet est un gigantesque réseau d'ordinateurs. Le Web est constitué par les milliards de documents dispersés sur des millions d'ordinateurs et qui circulent sur Internet. Ces documents sont reliés les uns aux autres selon le principe de l'hypertexte : désormais, pour accéder à une information, il suffit de cliquer !

Tim Berners-Lee (à droite) et Vinton Cerf (à gauche) : l'un a inventé le Web, l'autre Internet.

VIDÉO 2:30

lienmini.fr/3389-203

2000

2008

Internet des objets

Aujourd'hui, ce ne sont plus seulement les humains qui sont connectés à Internet mais aussi toute sorte d'objets, des montres aux pacemakers en passant par des caméras et des ampoules. Depuis 2008, plus d'objets que d'humains sont connectés, donnant naissance à ce que l'on appelle l'« Internet des objets ». Selon les projections, en 2020, plus de 50 milliards d'objets seront connectés à Internet.

Aujourd'hui, tout type d'objet peut être connecté à Internet, comme ici, cette enceinte

1982

Arrivée d'Internet

Internet n'est pas apparu d'un coup mais a émergé dans les années 1980. C'est en 1982 que le protocole TCP/IP est standardisé et commence à être installé sur des réseaux d'ordinateurs interconnectés qui vont progressivement former l'Internet. Les premières utilisations commerciales apparaissent à la fin des années 1980 (par exemple, les fournisseurs d'accès) tandis qu'Arpanet n'est plus utilisé à partir de 1990.

Câble sous-marin véhiculant les données d'Internet. Grace à ces câbles, Internet est aujourd'hui un réseau étendu sur pratiquement toute la planète.

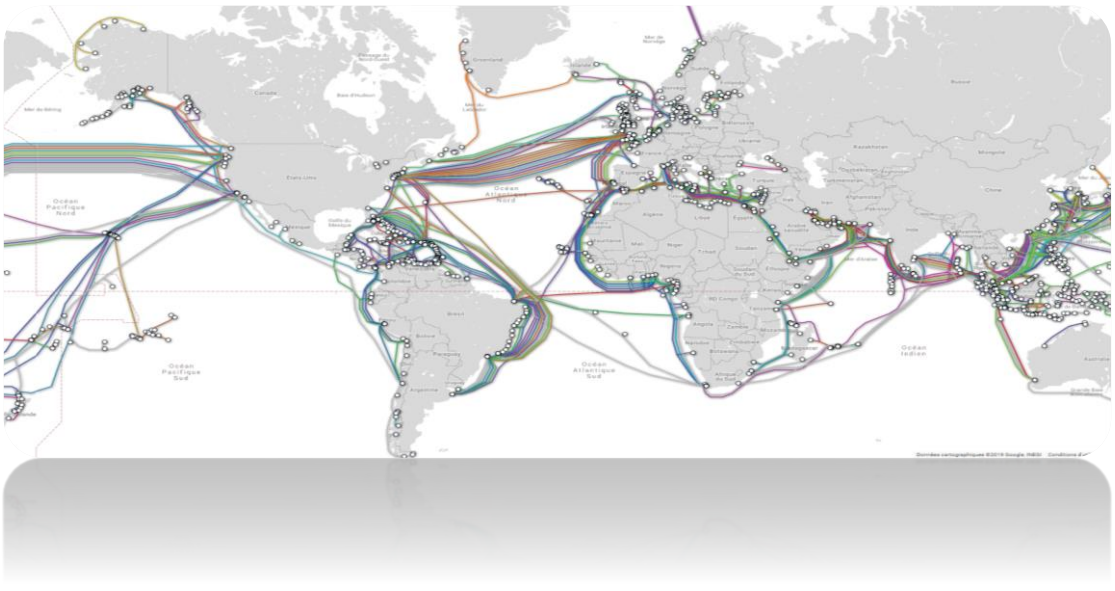
QUESTIONS

1. Quelle innovation a permis de garantir l'acheminement des données dans un réseau ?
2. À quoi servent les protocoles et dans quelle mesure ont-ils contribué au développement d'Internet ?
3. Quelle est la différence entre Internet et le Web ?

Voir DICO SNT p. 185

III- DEFINITION

« **Internet** est le réseau informatique mondial accessible au public. C'est un réseau de réseaux »



Et un réseau?

Un réseau est ensemble d'éléments interconnectés.

Un réseau peut être:

- « *matériel* » (comme le réseau électrique, le réseau routier, un réseau informatique…)
- « *immatériel* » comme le réseau social

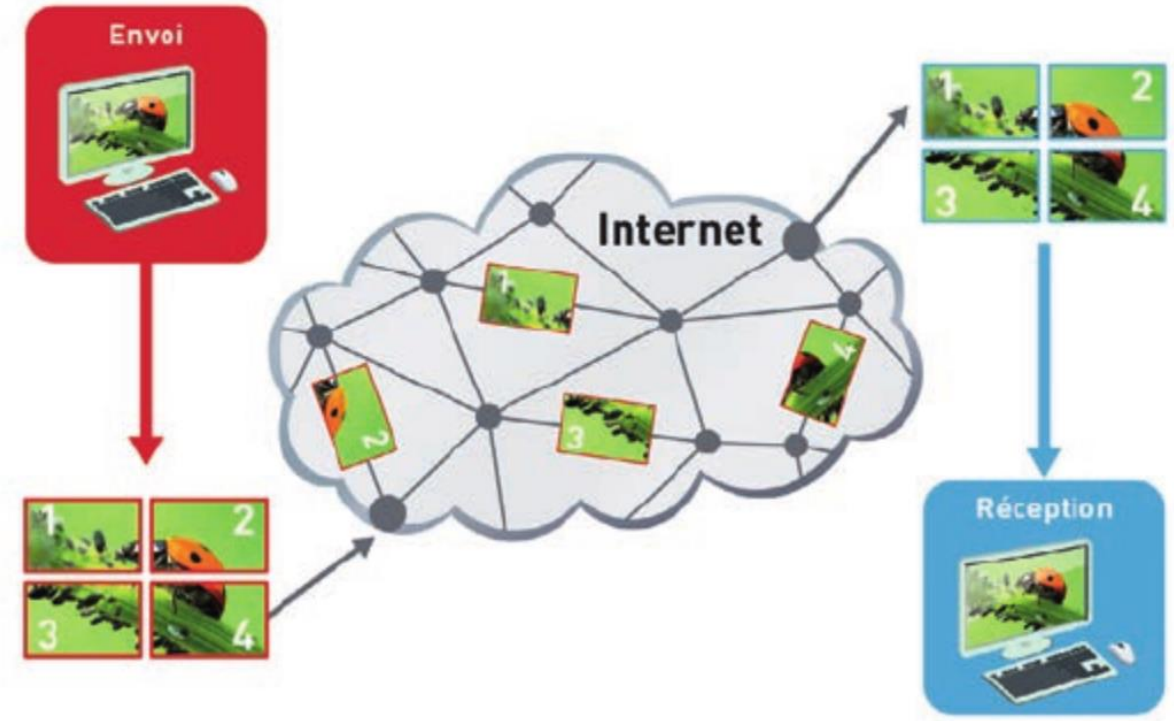
Les réseaux informatiques et Internet :	Internet, comment ça marche ? :
https://youtu.be/JqweQE6TDTc	https://youtu.be/L1Uz-46m2eI

RESUME

Ce qu'il faut savoir

- **Si l'on désire faire communiquer plusieurs ordinateurs entre eux, il faut que ces mêmes ordinateurs soient en réseau (tous les ordinateurs du lycée sont reliés entre eux, ils forment donc un réseau)**
- **Il est possible de relier des réseaux d'ordinateurs à d'autres réseaux d'ordinateurs, on obtient alors des réseaux de réseaux. Le réseau de réseaux le plus connu se nomme Internet**
- **L'idée de relier des réseaux d'ordinateurs à d'autres réseaux date des années 1970 (projet ARPAnet)**
- **Afin de pouvoir s'identifier, tout ordinateur possède une adresse sur un réseau : son adresse IP**
- **Les adresses IP sont de la forme : "a.b.c.d", avec a, b, c et d des nombres compris entre 0 et 255**

IV- Protocole TCP/IP



Pour que tous les éléments d'un réseau puissent se reconnaître, communiquer entre eux sans perdre les données et se comprendre, il est nécessaire d'établir des « **règles de communication** » ou « **protocoles** ».

Internet est un ensemble de réseaux qui utilisent le même protocole de communication **TCP/IP** : Transmission Control Protocol / Internet Protocol.

Le protocole TCP/IP permet de fragmenter les données à transmettre en paquets, à les envoyer au bon destinataire et à pouvoir ensuite les reconstituer dans l'ordre.

Mais qu'est-ce qu'un protocole ?

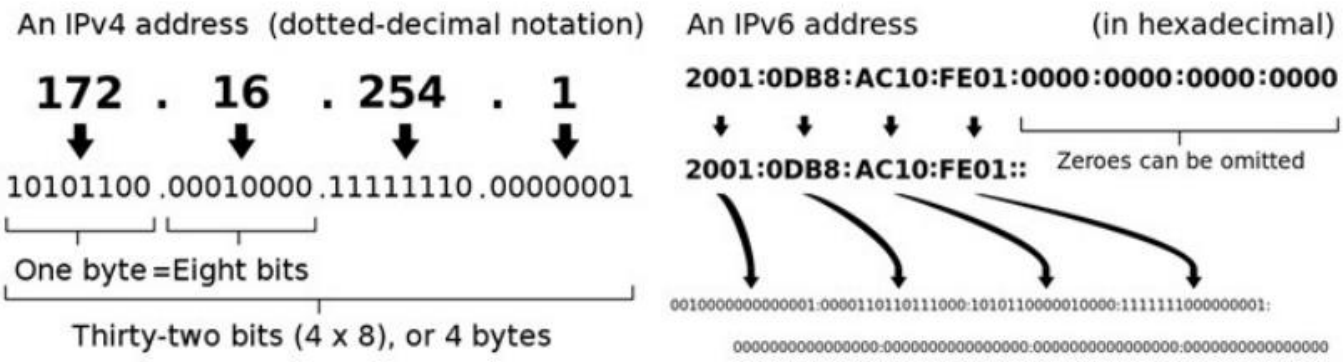
Un protocole de communication est un ensemble de contraintes permettant d'établir une communication entre deux entités (dans le cas qui nous intéresse 2 ordinateurs).

Il existe de nombreux protocoles qui permettent à deux ordinateurs de communiquer entre eux. Parmi ces nombreux protocoles, nous allons en étudier deux qui ont une importance fondamentale dans le fonctionnement d'internet : le protocole IP et le protocole TCP (d'un point de vue technique, les protocoles TCP et IP sont au cœur d'internet. Ils sont tellement liés entre eux que l'on parle souvent de protocole TCP/IP).

Le protocole IP

Le protocole IP permet d'attribuer une adresse et d'identifier tout appareil sur un réseau informatique utilisant le protocole IP (poste, imprimante, tablette, objet connecté, routeur, …). Il permet de déterminer les meilleurs chemins à travers les réseaux en fonction des adresses IP.

L'adresse IPv4 est actuellement codée sur 4 octets (de 0 à 255) soit 4 x 8 bits = 32 bits. Toutefois le nombre d'adresses possibles est limité à 4,3 Milliards et devient maintenant insuffisant. Une autre adresse IPv6 est utilisée, celle-ci codée sur 16 octets soit 128 bits.



Le protocole TCP e protocole TCP

Le protocole TCP est chargé de transporter et de contrôler le bon acheminement des données sur le réseau jusqu'à leur destination. Par exemple, il:

- établit la communication
- découpe les gros paquets de données en paquets plus petits et les numérote.
- à la réception, vérifie que les paquets sont bien arrivés et redemande l'envoi si nécessaire.
- envoie des accusés de réception.

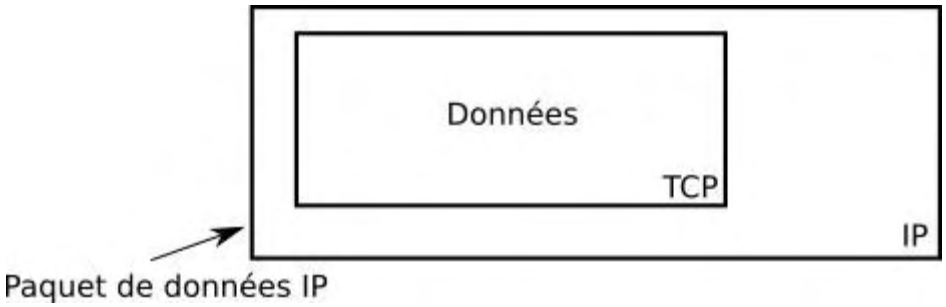
Une adresse IP

Une adresse IP est un numéro d'identification qui est attribué à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol

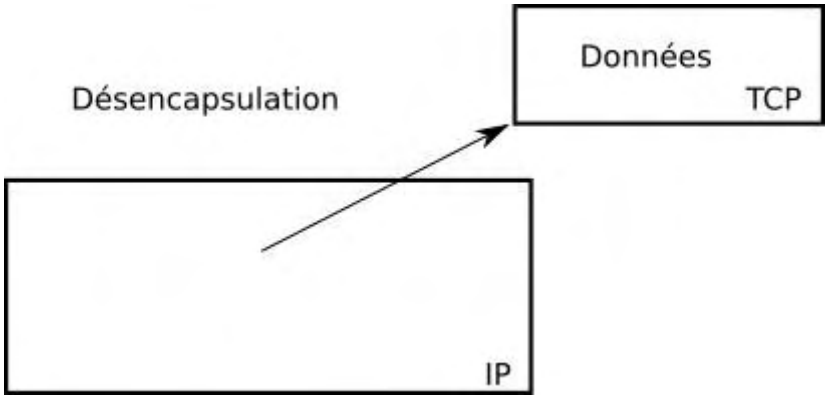
PRATIQUE

Quand un ordinateur A "désire" envoyer des données à un ordinateur B, après quelques opérations qui ne seront pas abordées ici, l'ordinateur A "utilise" le protocole TCP pour mettre en forme les données à envoyer.

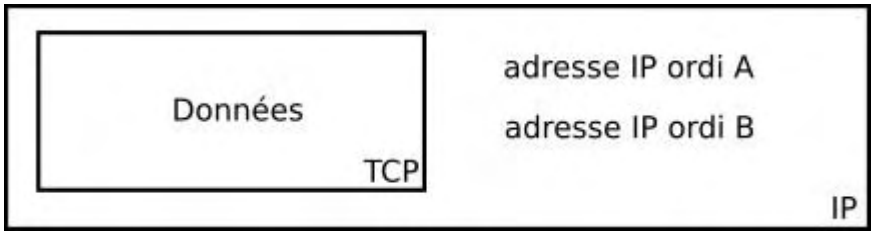
Ensuite le protocole IP prend le relai et utilise les données mises en forme par le protocole TCP afin de créer des paquets de données. Après quelques autres opérations qui ne seront non plus évoquées ici, les paquets de données pourront commencer leur voyage sur le réseau jusqu'à l'ordinateur B. Il est important de bien comprendre que le protocole IP "encapsule" les données issues du protocole TCP afin de constituer des paquets de données



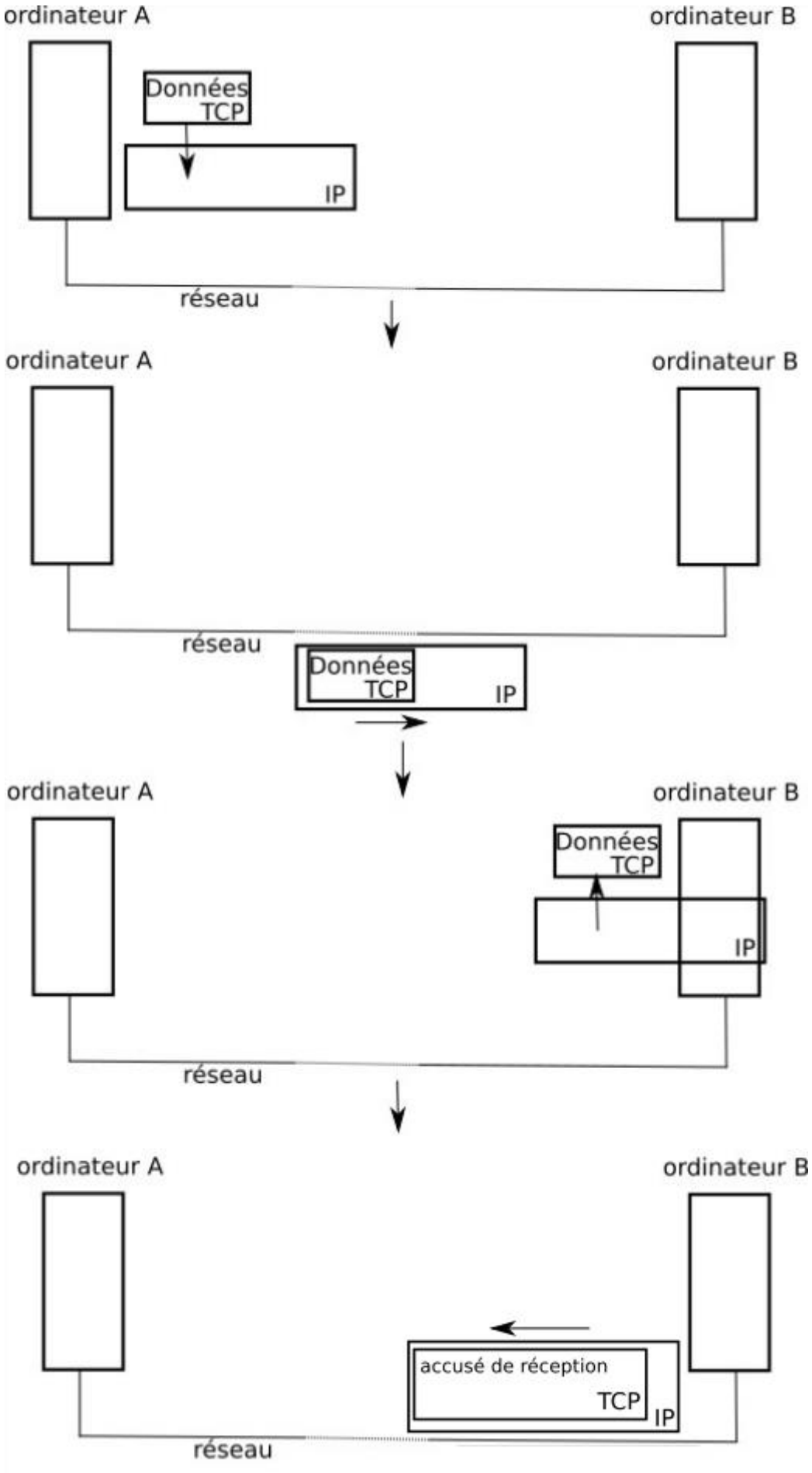
Une fois arrivées à destination (ordinateur B), les données sont "désencapsulées" : on récupère les données TCP contenues dans les paquets afin de pouvoir les utiliser.



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.



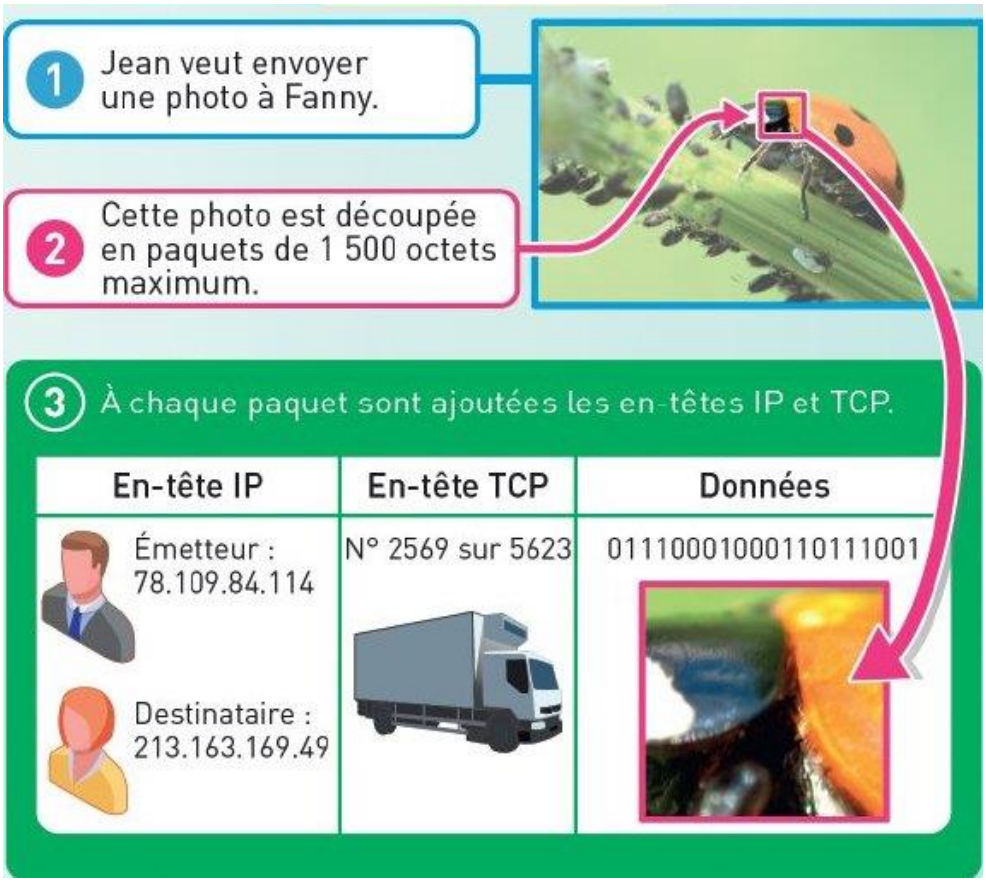
Le protocole TCP permet de s'assurer qu'un paquet est bien arrivé à destination. En effet quand l'ordinateur B reçoit un paquet de données en provenance de l'ordinateur A, l'ordinateur B envoie un accusé de réception à l'ordinateur A (un peu dans le genre "OK, j'ai bien reçu le paquet"). Si l'ordinateur 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. Nous pouvons donc résumer le processus d'envoi d'un paquet de données comme suit :


ordinateur A
ordinateur B
Données
TCP
IP
réseau
ordinateur A
ordinateur B
réseau
Données
TCP
IP
ordinateur A
ordinateur B
Données
TCP
IP
réseau
ordinateur A
ordinateur B
accusé de réception
TCP
IP
réseau

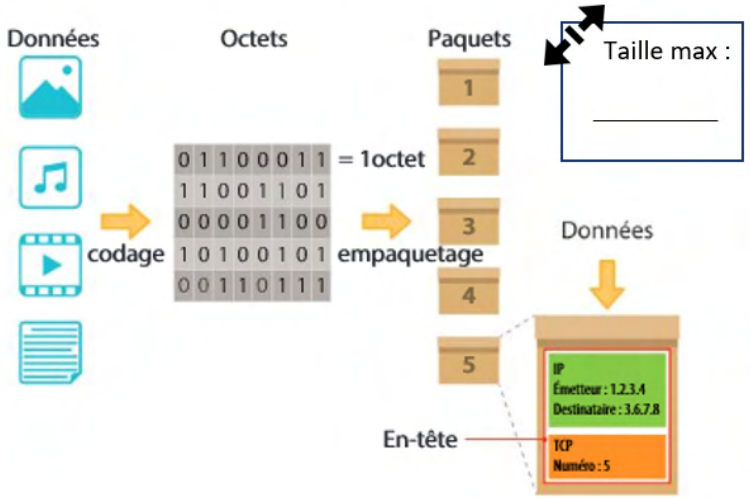
À noter qu'il existe aussi le protocole **UDP** qui ressemble beaucoup au protocole TCP. La grande différence entre **UDP** et TCP est que le protocole UDP ne gère pas les **accusés de réception**. Les échanges de données avec **UDP** sont donc moins fiables qu'avec TCP (un paquet "perdu" est définitivement "perdu" et ne sera pas renvoyé) mais beaucoup plus rapides (puisqu' il n'y a pas d'accusé de réception à transmettre). **UDP** est donc très souvent utilisé pour les échanges de données qui doivent être rapides, mais où la perte d'un paquet de données de temps en temps n'est pas un gros problème (par exemple le streaming vidéo).

Le protocole TCP/IP permet de fragmenter les données ou fichier (son, photo, vidéo ou texte...) à transmettre en paquets, à les envoyer au bon destinataire et à pouvoir ensuite les reconstituer dans l'ordre.

Si un des paquets n'arrive pas à destination, le fichier ne pourra pas être reconstitué, le paquet "perdu" devra être renvoyé par l'émetteur (voir le système d'accusé de réception décrit ci-dessus).



Quel **Protocole** permet de communiquer sur le réseau ? _____



Le protocole **IP** permet _____

_____

et ajoute _____

_____

Le protocole **TCP** permet _____

_____

_____

Comment savez-vous qu'un paquet n'est jamais arrivé à destination ?

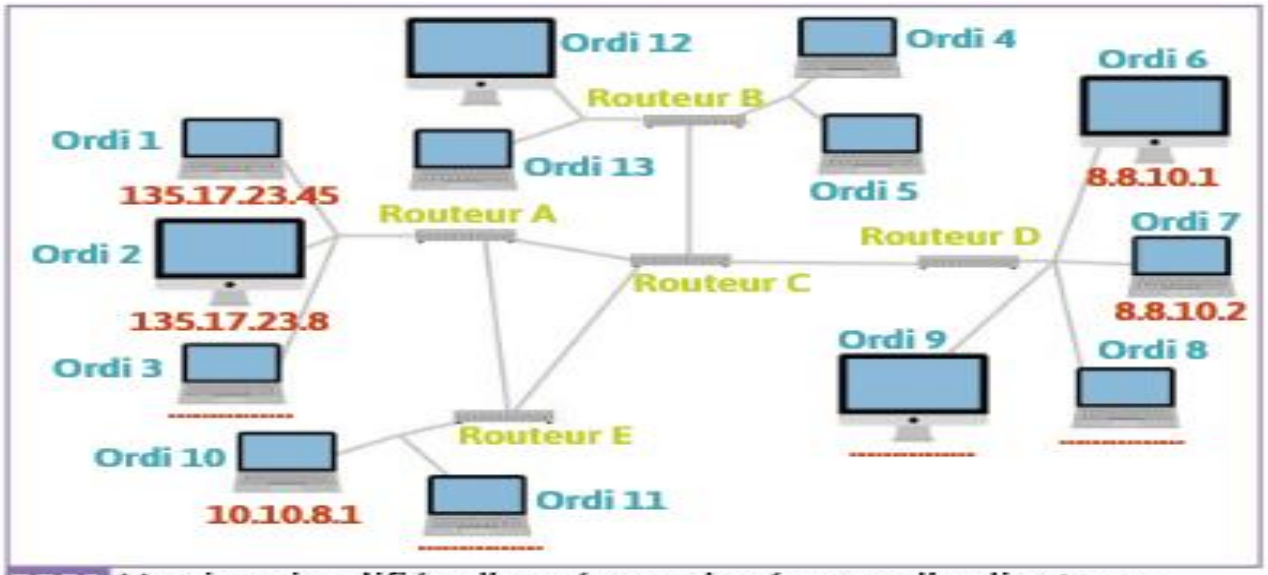
Que feriez-vous si un élément n'arrive pas à destination (pas d'accusé de réception) ?

Que devient un paquet qui se perd et qui ne trouve pas sa destination, est-ce qu'il ère à l'infini sur la toile ?

Ce qu'il faut savoir faire

- Connaissant le schéma d'un réseau, être capable de trouver une route entre 2 ordinateurs
- Travailler sur les adresses IP des ordinateurs : 2 ordinateurs appartiennent-ils au même réseau local ? Déterminer une adresse IP possible pour un ordinateur sur un réseau local connaissant l'adresse IP d'un autre ordinateur présent sur le même réseau local.

V- Le routage des paquets



DOC 1 Version simplifiée d'un réseau de réseaux d'ordinateurs

Le routage

Le routage est le mécanisme par lequel des chemins sont sélectionnés pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires.

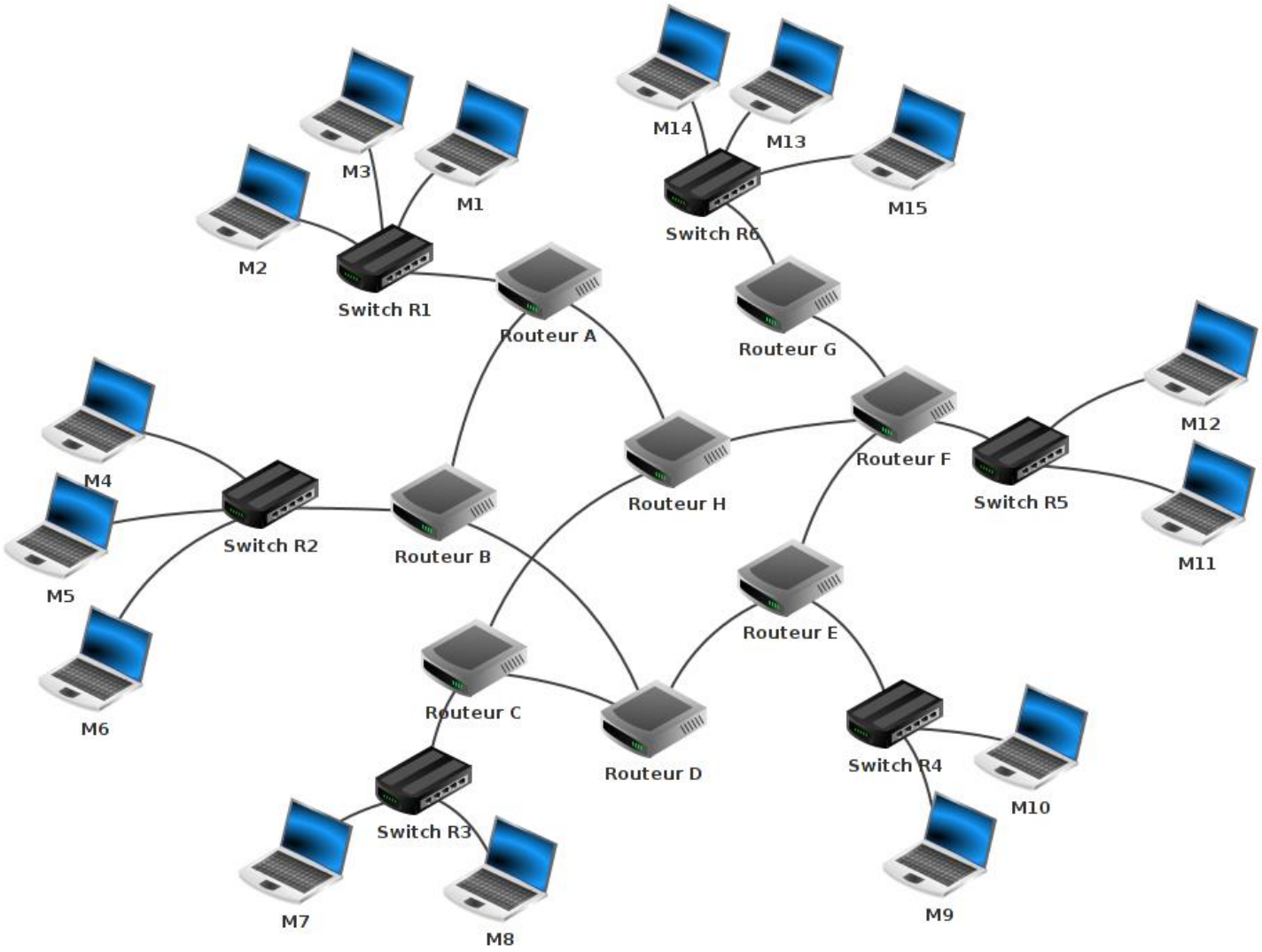
Les éléments du réseau qui s'occupent d'acheminer les paquets d'une extrémité à l'autre sont les routeurs :

Un **routeur** permet de relier ensemble plusieurs réseaux, il est composé d'un nombre plus ou moins important d'interfaces réseau (cartes réseau).

Précédemment, nous avons vu qu'internet est un « réseau de réseaux ». Nous avons aussi vu que les données sont transférées d'une machine à une autre sous forme de paquet de données.

Comment ces paquets de données trouvent leur chemin entre deux ordinateurs ?

Voici la représentation d'un « mini internet simplifié » :



Mini internet simplifié

Nous avons sur ce schéma les éléments suivants :

- 15 ordinateurs : M1 à M15
- 6 switchs (commutateur réseau) : R1 à R6
- 8 routeurs : A, B, C, D, E, F, G et H

Un switch est une sorte de « multiprise intelligente » qui permet de relier entre eux tous les ordinateurs appartenant à un même réseau, que nous appellerons "local" (nous verrons des exemples un peu plus bas).

Pour ce faire, un switch est composé d'un nombre plus ou moins important de prises **RJ45** femelles (un câble Ethernet (souvent appelé « câble réseau ») possède 2 prises **RJ45** mâles à ses 2 extrémités).

Différents switchs

Un routeur permet de relier ensemble plusieurs réseaux, il est composé d'un nombre plus ou moins important d'interfaces réseau (cartes réseau). Les routeurs les plus simples que l'on puisse rencontrer permettent de relier ensemble deux réseaux (ils possèdent alors 2 interfaces réseau), mais il existe des routeurs capables de relier ensemble une dizaine de réseaux.

Revenons maintenant à l'analyse de notre schéma :

Nous avons 6 réseaux locaux, chaque réseau local possède son propre switch (dans la réalité, un réseau local est souvent composé de plusieurs switchs si le nombre d'ordinateurs appartenant à ce réseau devient important).

Les ordinateurs M1, M2 et M3 appartiennent au réseau local 1.

Les ordinateurs M4, M5 et M6 appartiennent au réseau local 2.

Nous pouvons synthétiser tout cela comme suit :

- réseau local 1 : M1, M2 et M3
- réseau local 2 : M4, M5 et M6

Activité 1

Complétez la liste ci-dessus avec les réseaux locaux 3, 4, 5 et 6

COMMUNICATION

Voici quelques exemples de communications entre 2 ordinateurs :

Cas n°1 : M1 veut communiquer avec M3

Le paquet est envoyé de M1 vers le switch R1, R1 "constate" que M3 se trouve bien dans le réseau local 1, le paquet est donc envoyé directement vers M3. On peut résumer le trajet du paquet par :

M1→R1→M3

Cas n°2 : M1 veut communiquer avec M6

Le paquet est envoyé de M1 vers le switch R1, R1 « constate » que M6 n'est pas sur le réseau local 1, R1 envoie donc le paquet vers le routeur A. Le routeur A n'est pas connecté directement au réseau localR2 (réseau local de la machine M6), mais il "sait" que le routeur B est connecté au réseau local 2. Le routeur A envoie le paquet vers

le routeur B. Le routeur B est connecté au réseau local 2, il envoie le paquet au Switch R2. Le Switch R2 envoie le paquet à la machine M6.

M1 → R1→ Routeur A → Routeur B → R2 → M6

Cas n°3 : M1 veut communiquer avec M9

M1 → R1 → Routeur A → Routeur B → Routeur D → Routeur E → R4 → M9

Restons sur ce cas n°3 : comme vous l'avez peut-être constaté, le chemin donné ci-dessus n'est pas l'unique possibilité, en effet on aurait pu aussi avoir :

M1 → R1 → Routeur A → Routeur H → Routeur F → Routeur E → R4 → M9

Il est très important de bien comprendre qu'il existe souvent plusieurs chemins possibles pour relier 2 ordinateurs :

Cas n°4 : M13 veut communiquer avec M9

Nous pouvons avoir :

M13 → R6 → Routeur G → Routeur F → Routeur E → R4 → M9

ou encore : **M13 → R6 → Routeur G → Routeur F → Routeur H → Routeur C → Routeur D → Routeur E → R4 → M9**

On pourrait penser que le chemin "**Routeur F → Routeur E**" est plus rapide et donc préférable au chemin "**Routeur F → Routeur H**", cela est sans doute vrai, mais imaginez qu'il y ait un problème technique entre le Routeur F et le Routeur E, l'existence du chemin "**Routeur F → Routeur H**" permettra tout de même d'établir une communication entre M13 et M9. Parfois, on entend certains politiciens ou journalistes évoquer « **la coupure d'internet** », peut être comprendrez-vous mieux maintenant que cela n'a aucun sens, car même si une autorité quelconque décidait de couper une partie des infrastructures, les paquets pourraient passer par un autre chemin.

Activité 2

Déterminer un chemin possible permettant d'établir une connexion entre la machine M4 et M14.

On peut se poser la question : ***comment les switchs ou les routeurs procèdent pour amener les paquets à bon port***.

Sans entrer dans les détails, car cela dépasse notre objectif, vous devez tout de même savoir qu'ils utilisent **les adresses IP des ordinateurs**.

Nous avons vu qu'une adresse IP était de la forme a.b.c.d (exemple : 192.168.1.5). Une partie de l'adresse IP permet d'identifier le réseau auquel appartient la machine et l'autre partie de l'adresse IP permet d'identifier la machine sur ce réseau.

Exemple : Soit un ordinateur M4 ayant pour adresse IP **192.168.2**.1

Dans cette adresse IP "**192.168.2**" permet d'identifier le réseau (on dit que la machine M4 appartient au réseau ayant pour adresse 192.168.2.0) et "1" permet d'identifier la machine sur le réseau (plus précisément sur le réseau 192.168.2.0). M4, M5 et M6 sont sur le même réseau, l'adresse IP de M5 devra donc commencer par "**192.168.2**" (adresse IP possible pour M5 : 192.168.2.2). En revanche M7 n'est pas sur le même réseau que M4, M5 et M6, la partie réseau de son adresse IP ne pourra pas être "**192.168.2**" (IP possible pour M7 : 192.168.3.1).

En analysant la partie réseau des adresses IP des machines souhaitant rentrer en communication, les switchs et les routeurs sont capables d'aiguiller un paquet dans la bonne direction.

Imaginons que le switch R2 reçoive un paquet qui est destiné à l'ordinateur M7 (adresse IP de M7 : 192.168.3.1). R2 "constate" que M7 n'est pas sur le même réseau que lui (R2 appartient au réseau d'adresse 192.168.2.0 alors que M7 appartient au réseau d'adresse 192.168.3.0), il envoie donc le paquet vers le routeur B...

Activité 3

En partant des exemples ci-dessus, donnez une adresse IP possible pour les ordinateurs suivants :

M1 (en partant du principe que l'adresse de M2 est 192.168.1.3),

M6 (en partant du principe que l'adresse de M4 est 192.168.2.1) et

M8 (en partant du principe que l'adresse de M7 est 192.168.3.1).

Attention, les adresses IP (a.b.c.d) n'ont forcément pas les parties a, b et c consacrées à l'identification du réseau et la partie d consacrées à l'identification des machines sur le réseau : on rajoute souvent à l'adresse IP un "/" suivit du nombre 8, 16 ou 24

- si ce nombre est 8 (exemple : 192.168.2.1/8), cela signifie que pour une adresse a.b.c.d/8, la partie a est consacrée à l'adresse réseau, le reste (b, c, d) est consacré à la partie machine de l'adresse IP. On aura donc une adresse réseau de la forme a.0.0.0
- si ce nombre est 16 (exemple : 192.168.2.1/16), cela signifie que pour une adresse a.b.c.d/16, les parties a et b sont consacrées à l'adresse réseau, le reste (c, d) est consacré à la partie machine de l'adresse IP. On aura donc une adresse réseau de la forme a.b.0.0

- si ce nombre est 24 (exemple : 192.168.2.1/24), cela signifie que pour une adresse a.b.c.d/24, les parties a, b et c sont consacrées à l'adresse réseau, le reste (d) est consacré à la partie machine de l'adresse IP. On aura donc une adresse réseau de la forme a.b.c.0

Activité 4

Soit un ordinateur A d'adresse IP 172.15.22.3/16 et un ordinateur B d'adresse IP 172.16.22.4/16. Les ordinateurs A et B sont-ils sur le même réseau local ? Justifiez votre réponse

Activité 5

A et B sont 2 ordinateurs se trouvant sur le même réseau local. Sachant que l'adresse IP de A est 5.3.2.1/8, donnez une adresse IP possible pour B

Il est possible d'avoir autre chose que /8, /16 ou /24 (on peut par exemple trouver /10 ou /17...), mais ces cas font intervenir la notion de masque de sous-réseau qui n'est pas au programme de SNT.

Chose très importante à toujours avoir à l'esprit, même une simple photo n'est pas "transportée" en une fois d'un ordinateur A vers un ordinateur B. Les données correspondantes à la photo sont "découpées" en plusieurs morceaux, chaque morceau étant transporté par l'intermédiaire d'un paquet IP.

Les paquets IP transportant les "morceaux de photo" n'empruntent pas tous le même "chemin" pour aller de l'ordinateur A vers l'ordinateur B. Par exemple, pour aller de l'ordinateur M14 à M7, certains paquets passeront par les routeurs G, F, H et C alors que d'autres paquets emprunteront le chemin G, F, E, D et C.

Une fois que tous les paquets sont arrivés à destination, l'image originale peut être reconstituée. Si un paquet se "**perd**" en route, au bout d'un moment, il peut être renvoyé par la machine émettrice (voir le protocole TCP), pourquoi pas en empruntant un autre "chemin".

FICHE DE REVISION

Internet - Routage

• Pour être sur le même réseau local, 2 ordinateurs devront avoir la partie réseau de leurs adresses IP identique (exemple : A adresse IP 192.168.2.1/24 ; B adresse IP

192.168.3.2/24 => les ordinateurs A et B ne se trouvent pas sur le même réseau local)

Ce qu'il faut savoir

• Un switch permet de relier entre eux tous les ordinateurs appartenant à un même réseau local

• Un routeur permet de relier ensemble plusieurs réseaux locaux

• Si un ordinateur A veut envoyer des données un ordinateur B et si A et B n'appartiennent pas au même réseau local, les données devront transiter par un routeur.

• Dans un réseau, 2 ordinateurs ne peuvent pas avoir la même adresse IP

Une partie de l'adresse IP permet d'identifier le réseau auquel appartient la machine et l'autre partie de l'adresse IP permet d'identifier la machine sur ce réseau (exemples : 192.168.2.1/8 => 192 partie réseau – 168.2.1 partie machine ;

192.168.2.1/16 => 192.168 partie réseau – 2.1 partie machine ; 192.168.2.1/24 => 192.168.2 partie réseau – 1 partie machine)

Ce qu'il faut savoir faire

• Connaissant le schéma d'un réseau, être capable de trouver une route entre 2 ordinateurs

• Travailler sur les adresses IP des ordinateurs : 2 ordinateurs appartiennent-ils au même réseau local ? Déterminer une adresse IP possible pour un ordinateur sur un réseau local connaissant l'adresse IP d'un autre ordinateur présent sur le même réseau local.

VI- SIMULATION RESEAU

Après la théorie, passons maintenant à la pratique. Il est un peu difficile de mettre en place un réseau pour effectuer quelques tests. À la place nous allons utiliser un simulateur de réseau. Il existe différents types de simulateurs : du plus simple au plus "professionnel". Nous allons utiliser un simulateur relativement simple à prendre en main, mais suffisamment performant : Filius (la page web est en allemand, mais le logiciel est disponible en anglais).

Avant de visionner une petite vidéo qui devrait vous aider à prendre en main Filius, quelques petites indications

Nous allons utiliser deux commandes dans la vidéo :

- "**ipconfig**" qui permet de connaitre la configuration réseau de la machine sur laquelle est exécutée cette commande ("ipconfig" est une véritable commande sous Windows de Microsoft, sous les systèmes de type Unix (Linux ou macOS par exemple), la commande équivalente est "ifconfig")
- "**ping**" qui permet d'envoyer des paquets de données d'une machine A vers une machine B. Si la commande est exécutée sur la machine A, le "ping" devra être suivi par l'adresse IP de la machine B (par exemple, si l'adresse IP de B est "192.168.0.2", on aura "ping 192.168.0.2")

Autre chose à retenir, vous allez apercevoir dans cette vidéo un "**netmask**" (masque de réseau en français), vous devez juste savoir que :

- pour une adresse IP qui se termine par /8, on a un netmask qui est "255.0.0.0"
- pour une adresse IP qui se termine par /16, on a un netmask qui est "255.255.0.0"
- pour une adresse IP qui se termine par /24, on a un netmask qui est "255.255.255.0"

Vous pouvez maintenant visionner la vidéo

https://youtu.be/nzuRSOwdF5I?si=GyMlKD47Z-Ccuw-F (Filius 1, le lien est également sur PRONOTE)

Activité 1

En utilisant le logiciel Filius, créez un réseau de 4 machines (M1, M2, M3 et M4). L'adresse IP de la machine M1 est "192.168.1.1/24", choisissez les adresses IP des machines M2, M3 et M4.

Effectuez un "ping" de la machine M2 vers la machine M4.

Dans la vidéo ci-dessous, nous allons utiliser la commande "traceroute" : la commande "traceroute" permet de suivre le chemin qu'un paquet de données va suivre pour aller d'une machine à l'autre.

Vous pouvez maintenant visionner la vidéo

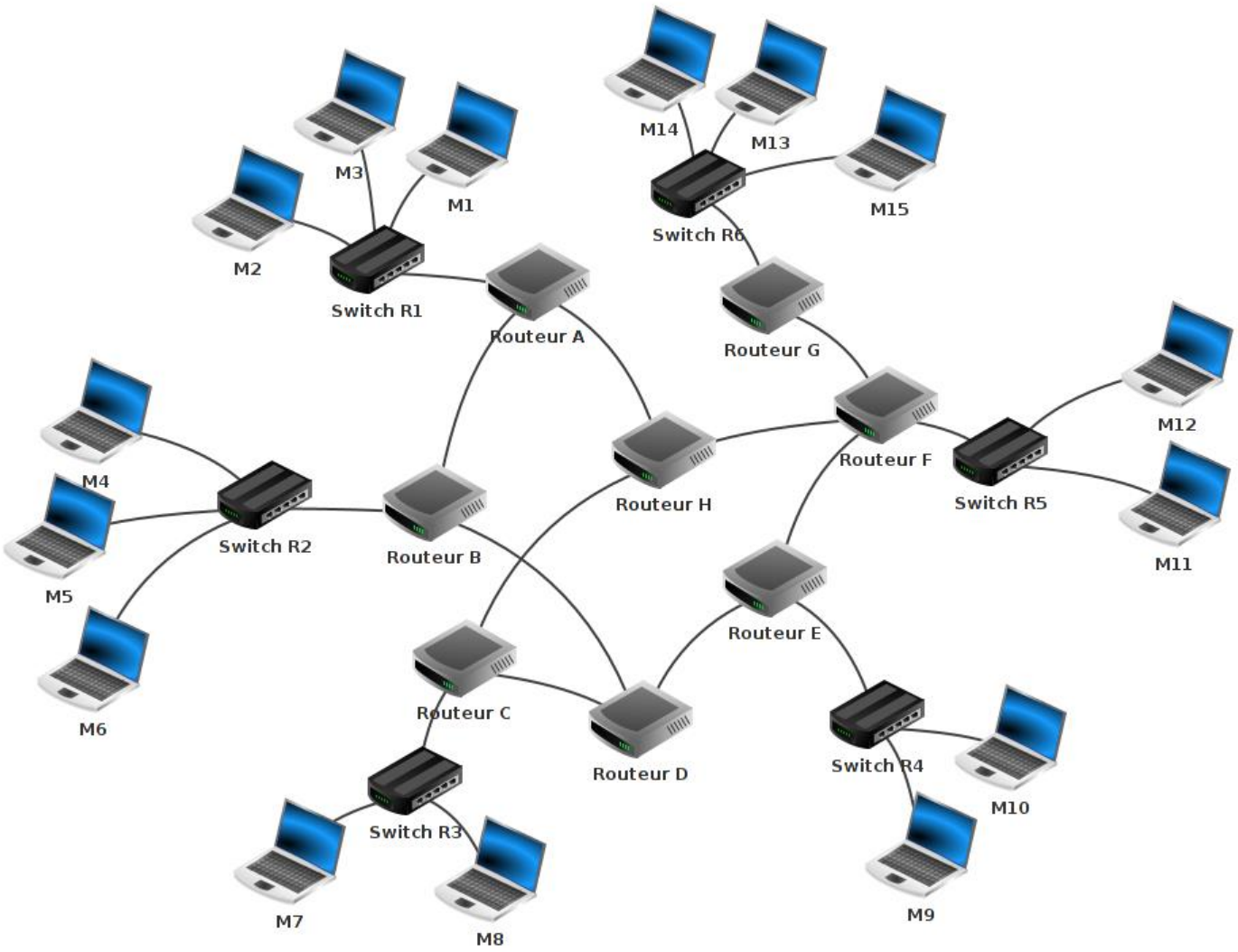
https://youtu.be/xyK6ThdQeR0?si=_N3X6lqE6ehu9OCN (Filius 2, le lien est également sur PRONOTE)

Activité 2

En utilisant le logiciel Filius, créez 3 réseaux de 2 machines chacun. Ces 3 réseaux seront reliés par un routeur. Après avoir effectué toutes les opérations de configuration nécessaires, effectuez un ping entre deux machines de deux réseaux différents.

Activité 3

Nous allons maintenant travailler sur un réseau plus complexe :



À l'aide du logiciel Filius, ouvrez le fichier snt_sim_res.fls.

Faites un "traceroute" entre l'ordinateur M14 et l'ordinateur M9 (n'oubliez pas de faire un "ipconfig" sur la machine M9 afin d'obtenir son adresse IP). Notez le chemin parcouru pour aller de la machine M14 à la machine M9.

Supprimez le câble réseau qui relie le routeur F au routeur E (simulation de panne), refaites un "traceroute" entre M14 et M9. Que constatez-vous ?

(ATTENTION : cela peut ne pas fonctionner du premier coup, car la mise à jour des tables de routage n'est pas immédiate : vous pouvez essayer de faire un ping entre M14 et M9, si cela ne fonctionne pas (timeout), attendez quelques secondes et recommencez. Une fois que le ping fonctionne, vous pouvez faire le traceroute).

VII- Adresses symboliques et serveurs DNS

Objectif :

- retrouver une adresse IP à partir d'une adresse symbolique et inversement.
- Connaitre la différence entre une adresse symbolique et une adresse IP.
- Comprendre le fonctionnement des adresses symboliques et des serveurs DNS,

Points clés :

- **Une adresse IP** est un numéro d'identification attribué par l'opérateur à chaque connexion sur internet.
- **Une adresse symbolique** est l'adresse que nous tapons dans la barre des tâches de notre navigateur pour chercher un site.
- **Le serveur DNS** permet de convertir un nom de domaine en adresse IP.

1. Adresse symbolique et adresse IP

Sur internet, mais aussi sur un réseau local (réseau fermé sans accès à internet), chaque machine (ordinateur, imprimante, etc.) dispose d'une adresse propre. Il existe 2 types d'adresses : **l'adresse symbolique et l'adresse IP.**

a. L'adresse symbolique

Une adresse symbolique également appelées noms de domaine est un ensemble de mots faciles à mémoriser qui permet de se connecter plus facilement à un site grâce au protocole de connexion **http://...**

On l'appelle aussi **adresse URL** :

> ***Exemple*** *:*
>
> *L'adresse symbolique du site yahoo.fr est http://www.yahoo.fr.*
>
> *"www.google.com" est une adresse symbolique*

Activité 1 : Citer quelques adresses symboliques que vous connaissez.

b. L'adresse IP

Une adresse IP est de la forme XXX.XXX.XXX.XXX. : il y a quatre séries de trois chiffres XXX au plus, séparées par des points.

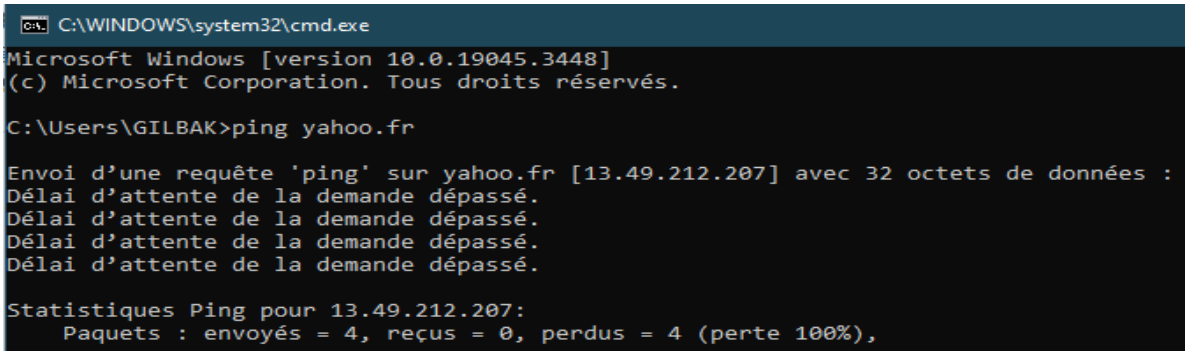
Remarque

Chaque paquet de XXX est un nombre compris théoriquement entre 0 et 255.

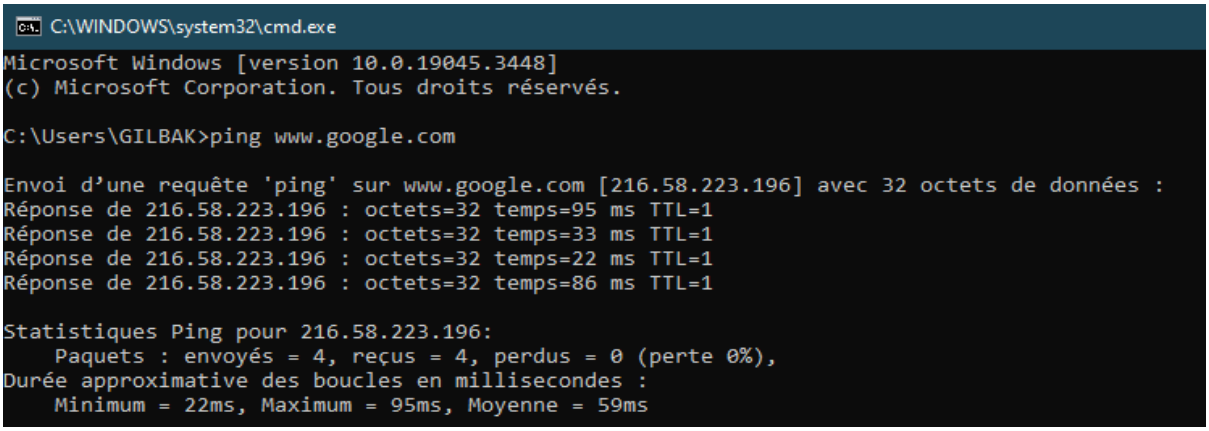
L'adresse IP permet l'identification d'une machine à l'intérieur d'un réseau.

Exemple :

L'adresse IP du site **yahoo.fr** est **13.49.212.207**



L'adresse IP du site *www.google.com* *est* ***216.58.223.196***



Activité 2 :

Essayez de trouver l'adresse IP de ces sites web m : "www.facebook.com", "www.wikipedia.org", en utilisant l'une des méthodes mentionnées précédemment, comme la commande "ping"

2. Serveur DNS

Pour faciliter l'usage pour les utilisateurs, un système de nommage symbolique a été défini pour associer des noms de domaine à des sites. La majorité des sites actuels possède donc un nom de domaine, aussi appelé alias DNS.

a. Définition et principe d'un alias DNS

Un alias DNS (ou nom de domaine) est un nom unique associé à l'adresse IP d'un serveur internet spécifique, comme la messagerie électronique, le service FTP de transfert de fichier, etc.

Internet utilise des serveurs DNS pour établir la correspondance entre l'adresse web symbolique d'un site et l'adresse IP du serveur qui héberge ce site. Ces serveurs DNS permettent ainsi aux utilisateurs un accès plus aisé aux ressources en ligne.

Un **serveur DNS** (Domain Name System) transforme les noms de domaine lisibles par l'homme (par exemple, google.fr) en adresses IP lisibles par une machine.

b. Comprendre les Serveurs DNS

Les serveurs DNS sont essentiels à l'Internet, car ils permettent de faire correspondre les adresses symboliques aux adresses IP correspondantes. Ils sont similaires à un annuaire téléphonique pour le web.

Exemple :

Imaginez que vous vouliez appeler un ami, mais vous ne connaissez que son nom. Vous utilisez alors l'annuaire téléphonique pour trouver son numéro de téléphone.

Remarque

L'annuaire permet en effet d'associer un numéro de téléphone à un abonné.

Les serveurs DNS font quelque chose de similaire en traduisant les adresses symboliques en adresses IP.

Exemple
On étudie le site internet https://www.aefe.fr.

- **L'adresse web symbolique** de ce site est https://www.aefe.fr;
- **L'alias DNS** (ou nom de domaine) de ce site est **aefe.fr**;
- **L'adresse IP** de ce site est **89.31.146.104**.

Lorsqu'un internaute saisit une adresse symbolique dans sa barre d'adresse, il effectue une requête au serveur DNS, lequel convertit cette adresse en une adresse IP qui est utilisable par tous les ordinateurs du réseau.

c. Intérêt d'un serveur DNS

Tous les fournisseurs d'accès à internet (Togo Télécom, société TEOLIS SA) disposent de leurs propres serveurs DNS, lesquels contiennent les adresses IP.

Lorsqu'on ouvre un navigateur tel que Chrome ou Firefox et qu'on accède à un site web, il est inutile de mémoriser et de saisir l'adresse IP. Il suffit d'entrer un nom de domaine comme google.fr pour arriver au bon endroit.

d. Retrouver une Adresse IP à partir d'une Adresse Symbolique

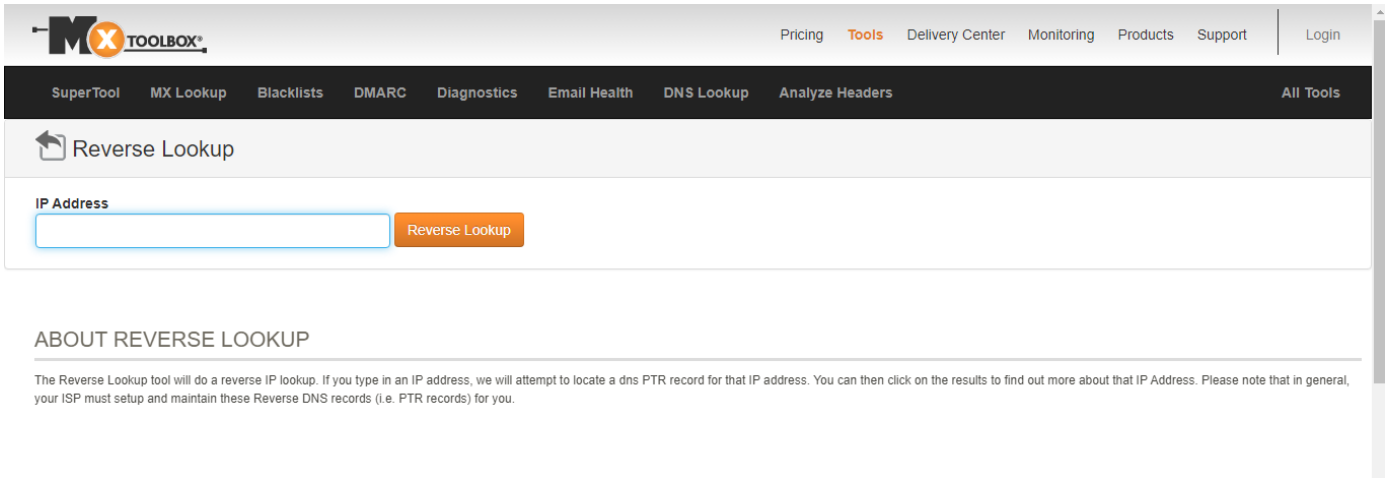
Parfois, il est utile de connaître l'adresse IP d'un site web pour diverses raisons, telles que la configuration réseau ou la résolution de problèmes.

e. Trouver une Adresse Symbolique à partir d'une Adresse IP

Parfois, il est nécessaire de retrouver l'adresse symbolique correspondant à une adresse IP.

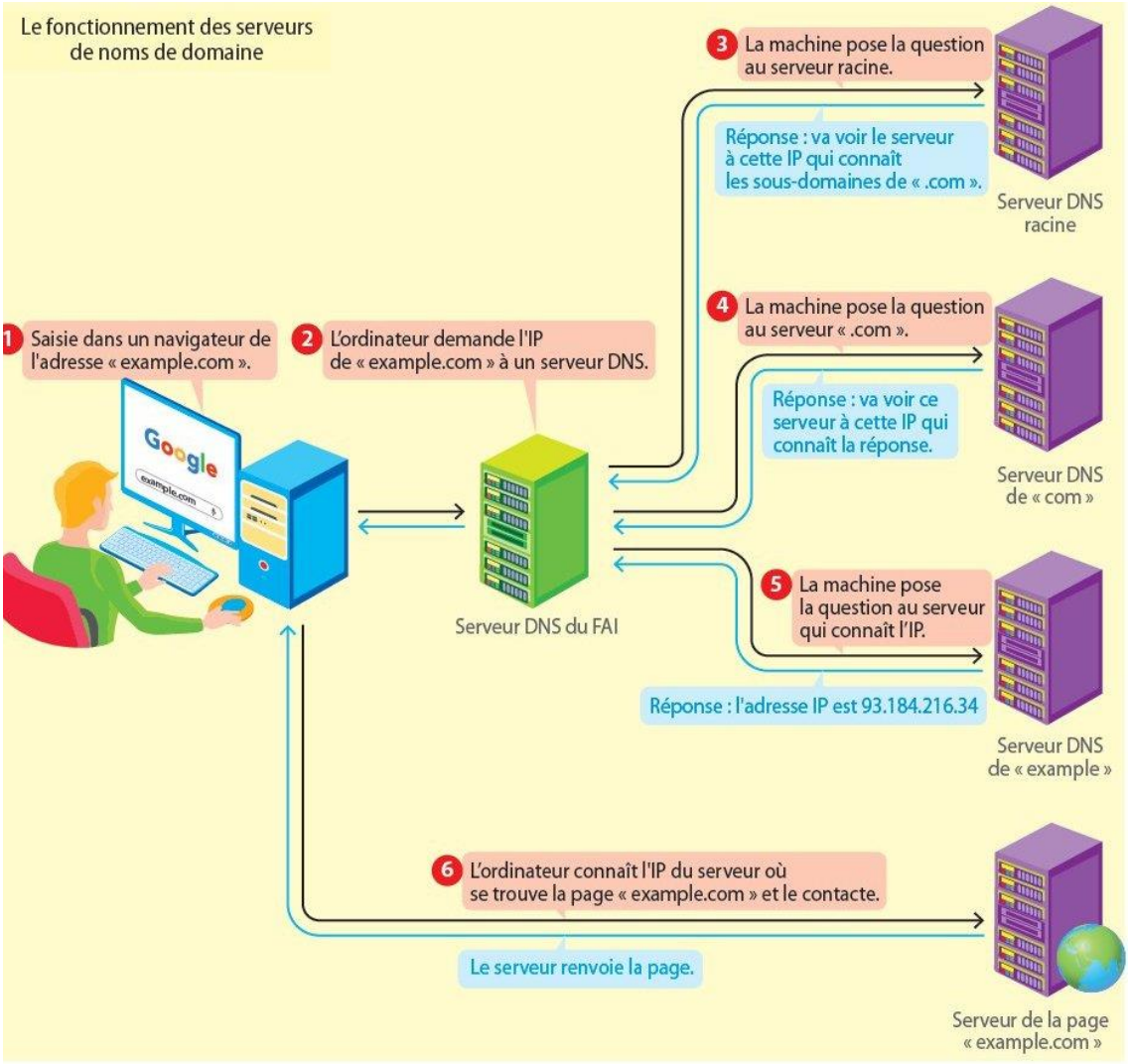
Activité 3 : Soit une adresse IP, par exemple : 216.58.213.206. Rechercher le nom de domaine associé en utilisant un outil en ligne de recherche DNS inverse.

NB : "https://mxtoolbox.com/ReverseLookup.aspx" pour effectuer cette recherche



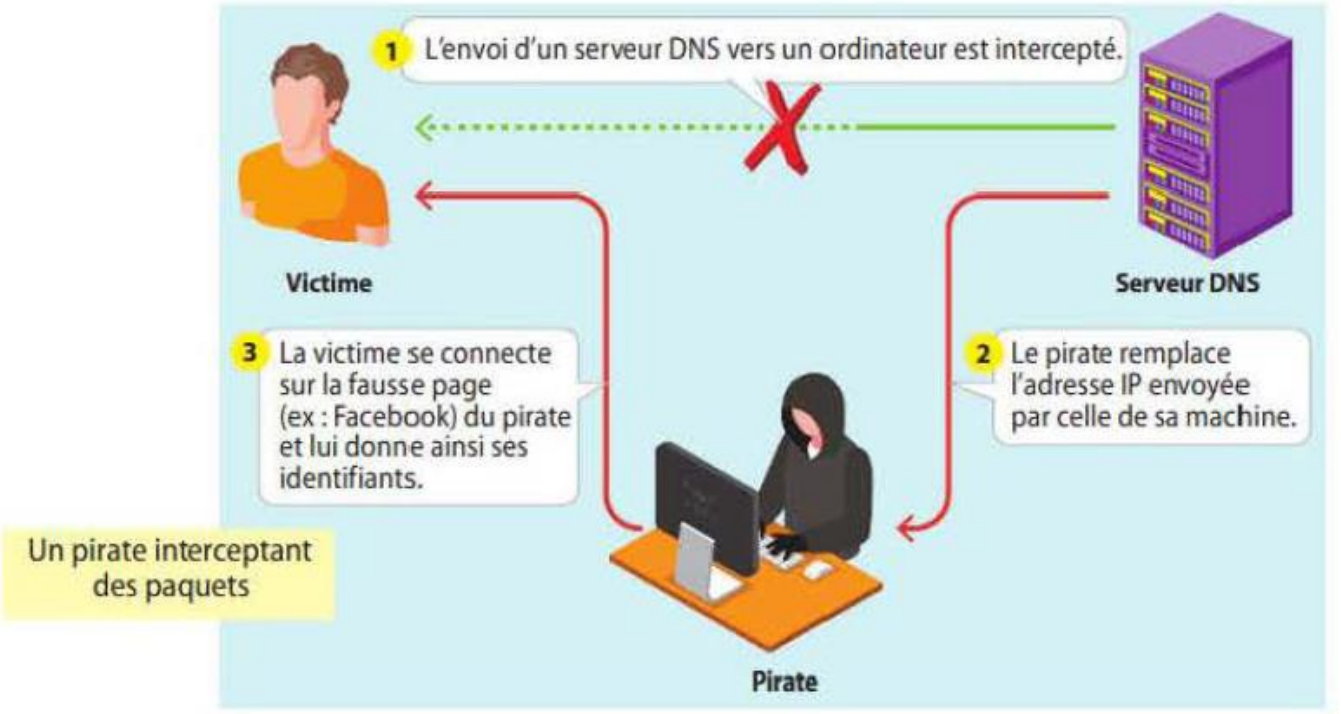
Lorsque vous tapez une adresse dans votre navigateur Web, comme «example.com», une requête est envoyée à un serveur de noms de domaine **(DNS)** qui détermine l'adresse IP de la machine hébergeant cette page sur le réseau.

Étant donné le grand nombre d'adresses sur le réseau, un serveur donné ne peut connaître qu'une partie de l'annuaire. Pour retrouver une adresse IP, il va communiquer avec d'autres machines qui connaissent d'autres parties de l'annuaire.



Le piratage d'un DNS

Pour communiquer entre elles, les machines qui permettent d'associer une IP à une adresse symbolique échangent des paquets d'informations. Si un pirate intercepte les paquets où se trouve une adresse IP. il peut remplacer celle-ci par l'IP de son ordinateur, ce qui lui permettra, par exemple de récolter des données personnelles.



Astuces :

Nom de domaine	Extension
IL est en Langage courant, est donc facile à retenir et constitue la conversion de l'adresse IP. **Exemples :** - Google - Wikipédia - Paris culture	C'est une indication de l'organisation qui gère Le site. L'extension peut être d'ordre technique ou géographique. **Exemples:** - .org pour les associations - .gouv pour les organisations gouvernementales - .com pour les sites commerciaux - .fr pour les sites français - .be pour les sites belges - .tg pour les sites togolais

Question :

À quel domaine appartient l'adresse www.education.gouv.fr ? Comment connaître l'adresse IP correspondante?

Réponse :

- L'adresse www.education.gouv.fr appartient au domaine de l'éducation en France et plus précisément au ministère de l'Éducation nationale, de la Jeunesse et des Sports. C'est le site officiel du ministère de l'Éducation en France.

- Pour connaître l'adresse IP correspondante du site, vous pouvez utiliser la commande "**ping**" dans l'invite de commande (sous Windows) ou "**traceroute**" (sous Linux ou macOS).

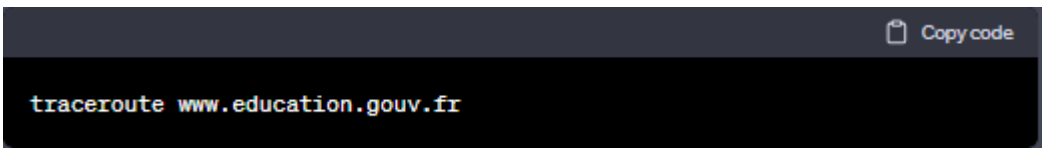
  Voici comment procéder :

Sous Windows :

1. Ouvrez l'invite de commande en appuyant sur la touche **"Windows"** + **"R"** pour ouvrir la boîte de dialogue **"Exécuter",** tapez **"cmd"** et appuyez sur Entrée.
2. Dans la fenêtre d'invite de commande, tapez la commande suivante et appuyez sur Entrée :

Sous Linux ou macOS :

1. Ouvrez le terminal.
2. Tapez la commande suivante et appuyez sur Entrée :



La commande "**ping**" ou "**traceroute**" affichera l'adresse IP du site web www.education.gouv.fr ainsi que le chemin que les paquets de données empruntent pour atteindre ce site.

Vous verrez une liste d'adresses IP, avec la première étant l'adresse IP du site en question. Cela vous permettra de connaître l'adresse IP correspondante de www.education.gouv.fr.

Exercice :

a. Quel est l'intérêt des adresses symboliques ?
b. Quelles sont les différences entre les adresses suivantes : www.wwf.fr , www.wwf.org, www.wwf.be, www.culture.gouv et www.hachette.com ?
c. À quoi sert un serveur DNS?

Ref : Page 22 Unité 3 ; Biblio Manuels

Ce qu'il faut savoir

• Chaque ordinateur est identifié sur le réseau uniquement par son adresse IP

• L'adresse IP étant difficile à retenir on associe souvent un ordinateur à un nom appelé adresse symbolique (par exemple " **aefe.fr** ")

• Un serveur DNS (Domain Name Server) est un serveur qui permet de transformer une adresse symbolique en adresse IP et vice versa

Ce qu'il faut savoir faire

Vous devez être capable de retrouver une adresse IP à partir d'une adresse symbolique et inversement (par exemple en utilisant le site https://mxtoolbox.com/ReverseLookup.aspx)

VIII- Les réseaux pair-à-pair

Objectif : *Décrire l'intérêt des réseaux pair-à-pair ainsi que les usages illicites qu'on peut en faire.*

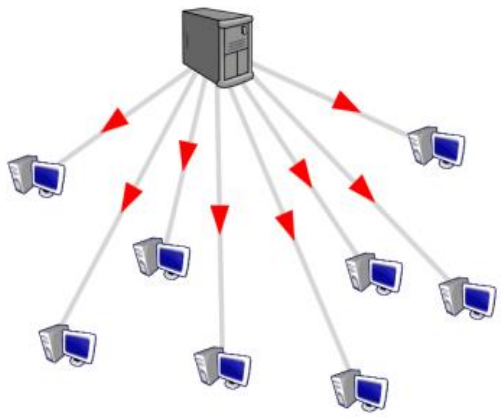
Il existe différentes utilisations d'Internet. On peut, par exemple, y chercher des informations hébergées sur des serveurs ou envoyer des courriels. On peut aussi y échanger des fichiers, comme le permettent les réseaux **pair-à-pair**, parfois en toute illégalité.

Ref : Page 27 Unité 5 ; Biblio Manuels

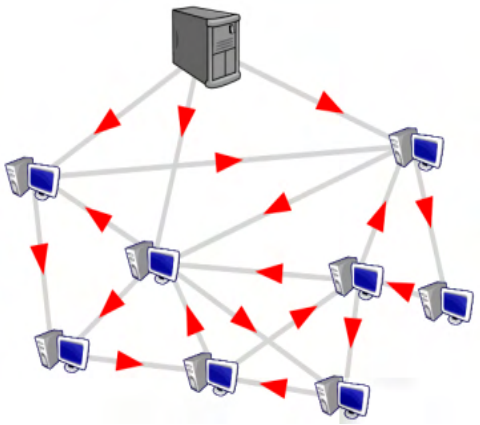
Quels usages et quelles limites pour le pair-à-pair ?

1- Les machines client et serveur

Dans un réseau pair-à-pair (de l'anglais peer-to · peer ou P2P), une machine est à la fois **client et serveur**. Elle peut envoyer des requêtes à d'autres machines comme elle peut y répondre. Pour cela, chaque machine est équipée d'un logiciel qui applique un protocole d'échange de données pair-à-pair avec d'autres machines munies du **même protocole**, formant ainsi un réseau pair-à-pair.



Réseau 1



Réseau 2

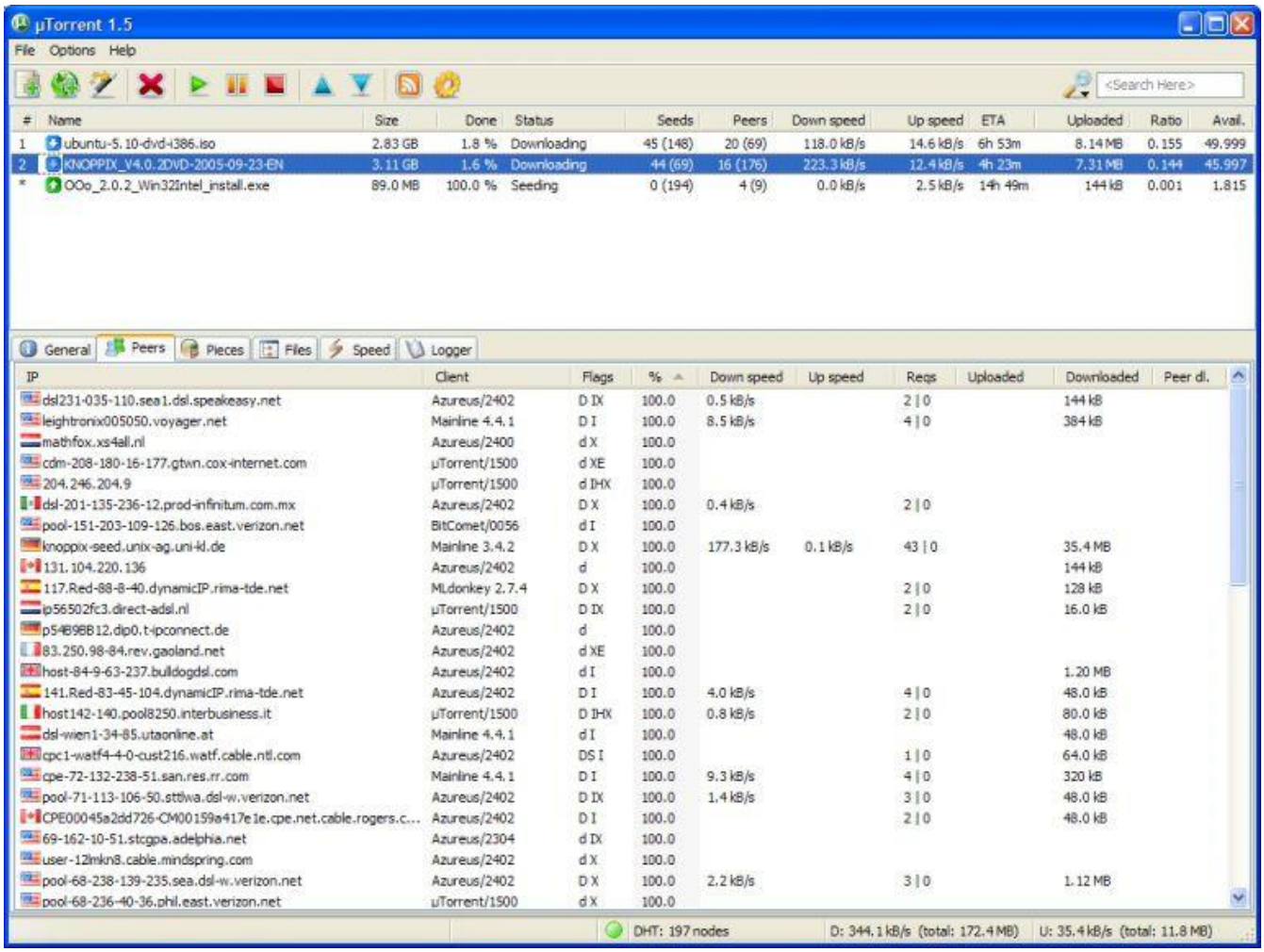
Le réseau 2 est pair-à-pair: chaque machine envoie et répond à des requêtes: elles sont donc à la fois client et serveur.

Le réseau 1 n'est pas pair-à-pair. Seule la machine centrale répond aux requêtes envoyées par les machines clients autour d'elle.

2- Le protocole BitTorrent

L'un des protocoles les plus connus d'échange de données sur un réseau pair · à-pair est le **BitTorrent**. Si l'on envoie une image par courriel, ses paquets sont transmis vers le récepteur depuis une source unique: l'ordinateur émetteur. Mais si l'on télécharge une image par BitTorrent, les paquets sont envoyés vers le récepteur depuis plusieurs sources, en l'occurrence tous les ordinateurs qui la possèdent en totalité ou en partie.

Le téléchargement est donc beaucoup plus rapide et si la liaison vers un ordinateur s'interrompt, un autre prend la suite.



3- Les usages légaux du pair-à-pair

L'usage légal le plus connu du pair-à-pair est le téléchargement de fichiers par des particuliers, mais aussi par des sociétés commerciales qui transmettent, par exemple, leurs mises à jour logicielles par ce biais. D'autres usages existent, comme le développement de réseaux sociaux pair-à-pair tels que Matrix. Au lieu que toutes les informations des utilisateurs soient centralisées sur les serveurs d'une société privée qui peut alors facilement les exploiter, elles sont décentralisées sur toutes les machines des utilisateurs et ainsi difficilement accessibles.

4- Les usages illégaux du pair-à-pair

L'usage illégal principal du pair-à-pair est le téléchargement gratuit d'œuvres culturelles normalement payantes : films, musique et jeux vidéo. En France, la **HADOPI** (Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet) veille aux intérêts des titulaires de droits d'œuvres protégées au titre de la propriété intellectuelle.

Le pair-à-pair est l'un des trois modes de piratage pour télécharger des vidéos, le streaming étant le moyen le plus utilisé désormais.

Quels sont les risques liés à l'utilisation d'un réseau pair à pair ?

• Instabilité : la gestion d'un réseau pair-à-pair étant dynamique, les pairs peuvent apparaitre et disparaitre à tout moment, par conséquent les ressources aussi.

L'inconvénient principal des réseaux pair-à-pair reste le comportement illicite de certains des utilisateurs.

- **Pratiques illégales** : non-respect des droits d'auteur, diffusion de contenus illégaux, etc.
- **La sécurité** : de nombreux virus circulent sur les réseaux pair-à-pair et rendent ces réseaux vulnérables.
- **le freeloading** : les freeloaders profitent des ressources partagées sur le réseau sans pour autant partager les leurs. Un réseau pair-à-pair ne peut fonctionner correctement que s'il y a participation active de tous leurs utilisateurs.
- **Contrôle des ressources** : dans un réseau pair-à-pair, les ressources circulent librement et sans contrôle ni vérification. Certaines ressources peuvent être corrompues, défectueuses ou erronées.
- **Le spoofing** : des entreprises privées indépendantes proposent de polluer les réseaux d'échanges de copies altérées de fichiers les plus populaires pour inciter les utilisateurs à revenir au téléchargement légal.
- **Vie privée** : certains réseaux pair-à-pair (centralisés) peuvent récupérer les adresses IP des utilisateurs, la vie privée des utilisateurs n'est alors plus protégée.
- **Régulation** : certains réseaux pair-à-pair garantissent l'anonymat des utilisateurs, il est donc plus difficile aux autorités d'appliquer les lois.
- **La propagande** : les réseaux pair-à-pair sont souvent envahis par des bannières publicitaires.

Qu'est- ce que le droit d'auteur?

Le droit d'auteur porte sur les œuvres de l'esprit (écrits, photos. partitions, logiciels, etc.) et confère à l'auteur un droit de propriété exclusif sur sa création, aussi bien en matière de droits moraux que patrimoniaux.

Que veut dire « en violation des droits d'auteur » ?

La violation des droits d'auteur est la reproduction, la diffusion d'œuvres sans s'acquitter des droits d'auteur. Les droits d'auteur sont les droits de tout auteur d'œuvres (musique, film, texte, photo, image, vidéo, design, textile…).

Ils sont de 2 types :

- **moraux** (c'est l'auteur qui décide quand il divulgue son œuvre, il peut réclamer que son nom y soit toujours associé, empêcher des détournements de ceux qui ne respectent pas son œuvre, le retrait de son œuvre auprès des personnes à qui il a cédé les droits d'exploitation) ;
- **patrimoniaux** : droit d'exploitation et de reproduction de l'œuvre. Ces droits sont généralement cédés aux diffuseurs contre rémunération à l'auteur.

A retenir

	Client-Serveur	Pair-à-Pair
Définition	Il y a un serveur spécifique et des clients spécifiques connectés au serveur.	Le client et le serveur font le même travaille. Chaque nœud agit en tant que client et serveur
Service	Le client demande le service et le serveur offre le service.	Chaque nœud peut demander des services et peut également fournir des services.
La stabilité	Modèle Client-Serveur est plus stable et évolutif.	Peer-to Peer souffre si le nombre de pairs augmente dans le système.
Le coût	Le client-serveur est coûteux à implémenter.	Peer-to-peer sont moins chers à mettre en œuvre.
Coté Serveur	Lorsque plusieurs clients demandent les services simultanément, un serveur peut être encombré.	Comme les services sont fournis par plusieurs serveurs répartis dans le système peer-to-peer, un serveur n'est pas encombré.
Les données	Les données sont stockées dans un serveur centralisé. Cela assure la sécurité des données.	Chaque pair a ses propres données. La capacité de stockage n'est donc pas limité et les données sont davantage disponibles.

IX- Indépendance d'internet par rapport au réseau physique

Objectif : *Caractériser quelques types de réseaux physiques : obsolètes ou actuels, rapides ou lents, filaires ou non. Caractériser l'ordre de grandeur du trafic de données sur internet et son évolution.*

1- L'évolution du trafic sur Internet

Chaque mois, il s'échange sur Internet de l'ordre de **168 millions de téraoctets (1 000 milliards d'octet) de données**. Un téraoctet représente la capacité de stockage moyen d'un gros disque dur. En 1990, ce chiffre était seulement de l'ordre de 1 téraoctet.

2- Les causes de l'évolution du trafic

La croissance du trafic sur Internet est principalement due à la diffusion de vidéos haute définition, suivie par la vidéo à la demande et le Web L'arrivée de la 5G avec un débit 100 fois supérieur à celui de la 4G va accentuer ce phénomène car il sera encore plus facile qu'aujourd'hui de regarder des vidéos HD sur son smartphone.

3- La communication entre machines

Les machines d'un **réseau informatique** sont connectées par différents moyens. Il faut distinguer les logiciels, qui gèrent les échanges de données, des machines sur lesquelles ils sont installés. En un sens, Internet est indépendant du réseau physique car les logiciels permettent de passer d'un type de connexion à un autre, assurant ainsi la continuité des communications. Par exemple, un smartphone peut passer du **Wifi** d'une box à la 4G d'une antenne.

Dans une maison et son voisinage, nombre d'appareils du quotidien sont connectés entre eux et à

Internet de diverses manières, filaires et non filaires. Ils forment ainsi un **réseau**.

A retenir :

Les ordinateurs sont reliés entre eux par divers liens qui peuvent être filaires (fibre optique, ADSL, etc.) ou sans fil (Wifi, Bluetooth, etc.) .

Internet est indépendant du réseau physique grâce à des protocoles de communication qui permettent de passer d'un type de connexion à un autre pour assurer la continuité des communications.

Exemple : Un smartphone peut se connecter à Internet en passant du Wifi d'une box à la 4G d'une antenne

Connexion avec fil	Connexion sans fil
Fibre optique : très haut débit, jusqu'à 100 mégaoctets/seconde	**4G :** pour la téléphonie, 10 à 20 mégaoctets/seconde
ADSL : utilise les lignes téléphoniques, environ 2,75 mégaoctets/seconde (dépend de la distance au relais téléphonique)	**Wifi :** jusqu'à 7 mégaoctets/seconde
	Bluetooth : pour connecter des appareils proches par ondes radios, 0,4 mégaoctet/seconde

Caractérisation de certains réseaux

Nom	Lignes téléphoniques RCT	Wifi	Bluetooth	ADSL	Fibre optique	4G	Satellite
Date d'apparition	1998	1999	1999	1999	2005	2008	2011
Type de liaison - équipement	Filaire Modem	Sans fil	Sans fil	Filaire Box ADSL	Filaire Box fibre	Sans fil	Sans fil
Nature du signal	Électrique	Ondes radio	Ondes radio	Électrique	Lumière	Ondes radio	Ondes radio
Portée de la communication	–	100 m	10 m	–	–	–	–
Débit théorique de la transmission	56 Kbit/s	54 Mbit/s	1 Mbit/s	25 Mbit/s	100 Mbit/s	25 Mbit/s	20 Mbit/s

Exemples de durée de téléchargement selon le débit :

	Modem	ADSL	VDSL	Fibre
Débit	36 kbit/s	16 Mbit/s	30 Mbit/s	1 Gbit/s
film de 500 Mo	1 jour et 7 h 36 min et 17 s	4 min 10 s	2 min 13 s	4 s
Mise à jour Mac de 10 Go	26 jours 23 h 16 min et 8 s	1 h 25 min 20 s	45 min 30 s	1 min 20 s

Internet en chiffres

- Le nombre d'internautes dans le monde est passé de **2 milliards** en 2011 à **4 milliards** en 2017 et devrait être de **5,5 milliards** en 2021.
- En 2011, **5 exaoctets** de données étaient générés tous les deux jours. Cela se fait en 2017 en 10 minutes seulement
- Il n'y avait que **130 exaoctets** de données dans l'univers numérique en 2005. Il devrait y en avoir plus de **40 000** à l'horizon 2020. Cette explosion est essentiellement due à la vidéo. Pour mieux visualiser: **1 exaoctet** équivaut à **250 millions de DVD**.
- En 2020, les données représenteront l'équivalent de plus de **5 000 Go** par personne.
- En 2012, environ 30 millions d'adresses IP sont attribuées aux *9* millions d'habitants de la Suède.

Au même moment, la Somalie compte environ 10 000 adresses IP pour plus de 10 millions d'habitants.

BILAN :

- Quels sont les types de réseaux existant sur Internet?
- Que diriez-vous de l'évolution du trafic des données sur internet?

Ce qu'il faut savoir

- Les réseaux pair-à-pair ou peer to peer en anglais (abréviation "p2p"), ne sont pas basés sur l'architecture client-serveur classique (voir le cours sur l'architecture client-serveur)
- Dans un réseau p2p chaque machine joue en même temps le rôle de client (elle demande des ressources à une autre machine) et le rôle de serveur (elle fournit des ressources à une autre machine)

- Il existe énormément de protocoles qui s'appuient sur des réseaux de pair-à-pair. La plupart de ces "protocoles p2p" sont destinés au partage de fichier, mais il est aussi possible de créer des systèmes de "calculs distribués" grâce au réseau p2p (répartir des calculs extrêmement complexes sur un grand nombre d'ordinateurs personnels)
- le protocole BitTorrent s'appuie sur les réseaux p2p. Il permet de partager des fichiers. Même si le protocole BitTorrent n'a rien d'illégal, il est souvent utilisé pour partager des fichiers (films, jeux…) de façon illégale..

Exercice

Tom veut envoyer une vidéo de 1Go à Farida uniquement équipée d'un smartphone 4G, en vacances à l'étranger.

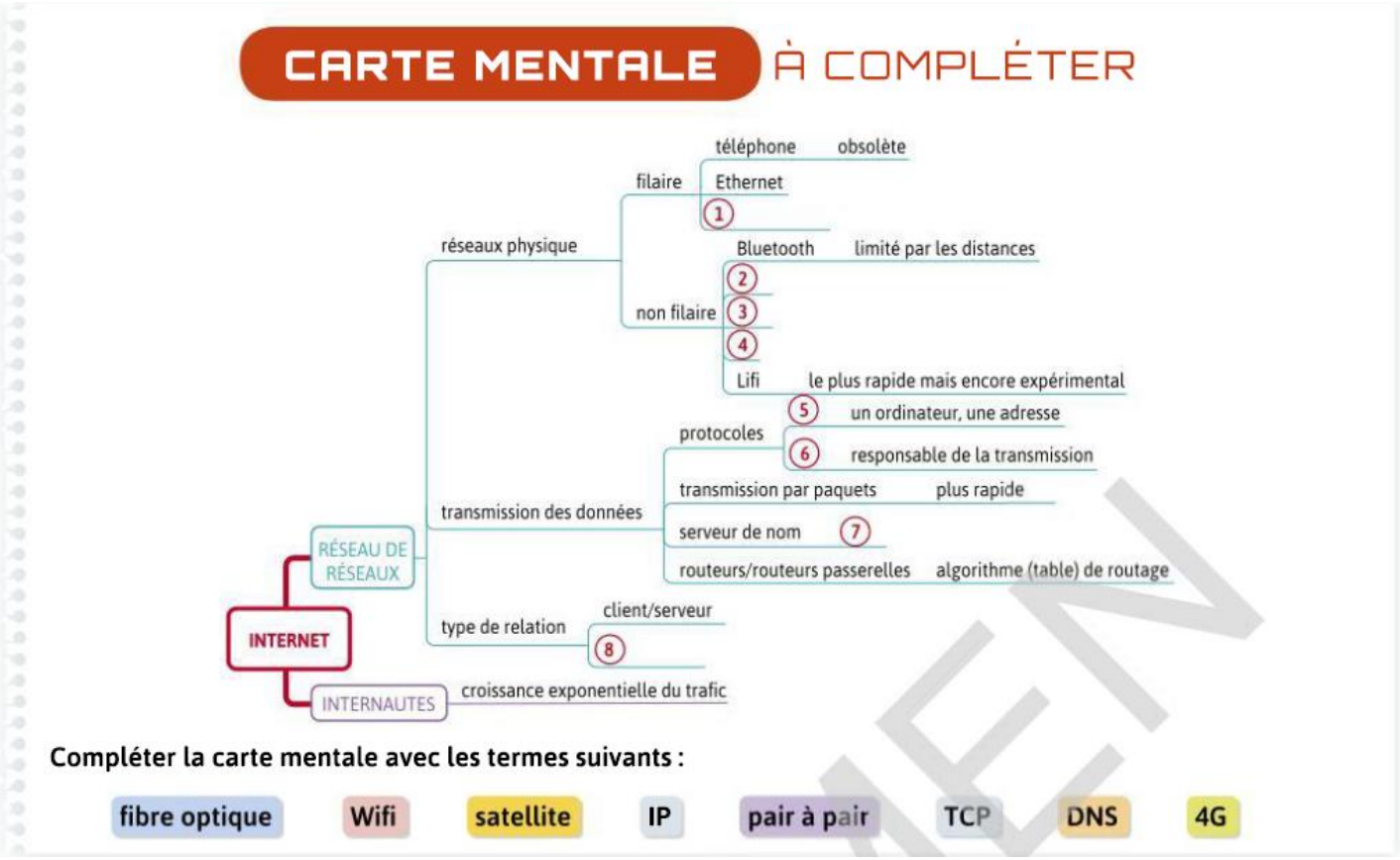
Question 1 :

En vous reportant à la double page « Internet en une image», quel type de connexion Tom peut-il utiliser pour envoyer sa vidéo?

Question 2 :

a- Calculer le temps de transmission du fichier, si Tom utilise son smartphone 4G (débit 25 Mbits/s), sa tablette connectée en Wifi (débit 54 Mbits/s) ou son ordinateur relié au réseau avec la fibre (débit 100 Mbits/s).

b- Calculer le temps de transmission avec les moyens disponibles en 1998.



Je retiens par le texte

1. Les réseaux informatiques

Internet est un **réseau** de réseaux d'ordinateurs où circulent des données. Les machines échangent des **requêtes.** Celles qui envoient les requêtes sont appelées **clients** et celles qui répondent **serveurs.** Leurs liens peuvent être filaires ou non.

2. La circulation des données sur Internet

Les informations circulant sur Internet sont découpées en **paquets** de bits. Chaque paquet reçoit en en-tête les adresses **IP** de son émetteur et de son destinataire. Cette dernière est utilisée par les **routeurs** répartis sur tout le réseau qui se transmettent ainsi les paquets jusqu'à leur destinataire. C'est ce **protocole** IP qui assure donc l'envoi des paquets aux bons endroits.

Les paquets reçoivent également un en-tête **TCP,** un protocole qui assure leur transport et leur intégrité.

3. L'annuaire d'Internet

Une adresse IP, une série de chiffres, correspond à une adresse symbolique, sous forme textuelle et vice-versa. La correspondance entre adresses IP et symbolique se trouve dans l'annuaire **DNS** un ensemble de données réparties sur des serveurs dans tout le réseau.

4. Les réseaux pair-à-pair

Dans un réseau **pair-à-pair** (P2P), les machines émettent et répondent à des requêtes d'autres machines : elles sont à la fois client et serveur. Le P2P est parfois utilisé pour échanger des fichiers de manière illégale.