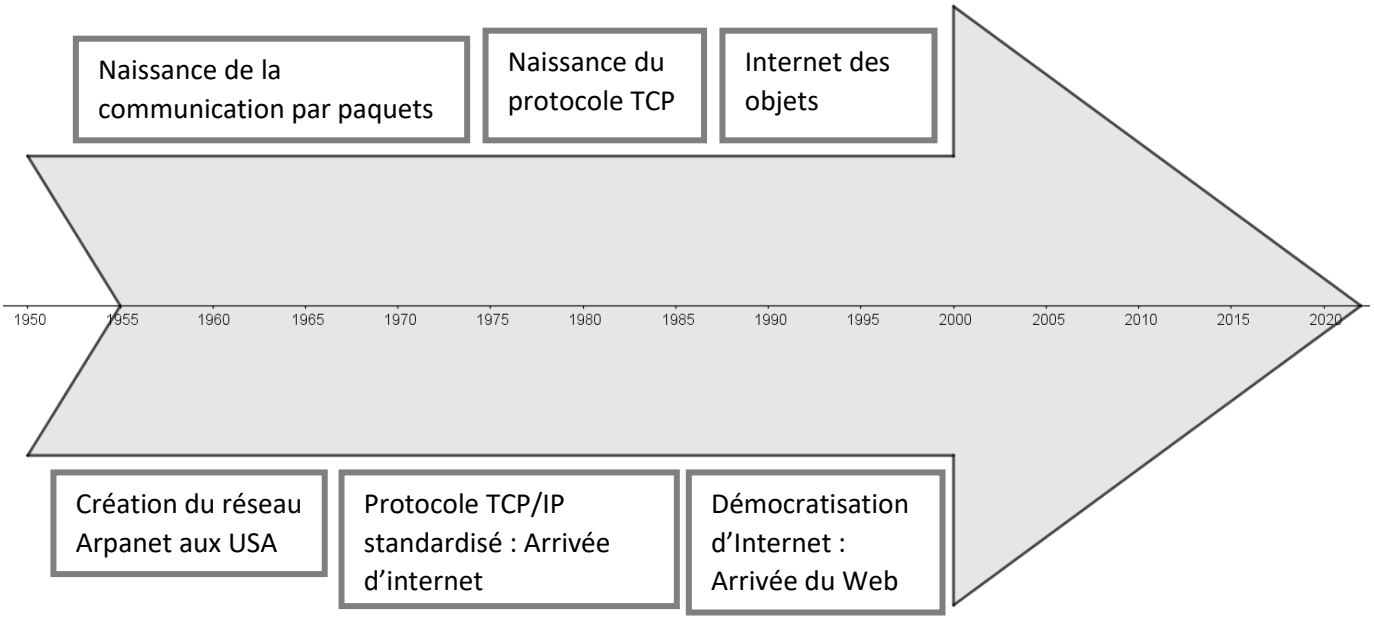
Seconde
Thème : Internet
Sciences Numériques et Technologie

Exercice n°1 : Repères historiques

Repérer les événements ci-dessous sur la frise chronologique.



Exercice n°2 : Les câbles sous-marins

►1. Inauguré en 2021, le câble Ellalink composé de 6 000 km de fibre optique, relie le Portugal au Brésil. Quel est le **temps de latence** c'est-à-dire le temps mis par les données pour faire un aller-retour à la vitesse de la lumière ?

►2. Quels nouveaux acteurs émergent sur le marché des câbles sous-marins ?

►3. Quel scandale a été révélé en 2021 par la TV danoise ?

►4. Qui est responsable de la sécurité des câbles sous-marins en France ? Est-ce vraiment possible de sécuriser plusieurs milliers de km de câbles ? Quelle stratégie est adoptée en France en conséquence ?

►5. Quelle est la durée de vie moyenne d'un câble sous-marin ?

A RETENIR :

Internet est un réseau de réseaux de machines dans lequel circulent des données. Les machines échangent des informations à l'aide de **requêtes**. Un ordinateur qui émet une requête est appelée un **client**, celui qui y répond, un **serveur**.

1. Réseau physique

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

2. La circulation des données, le protocole TCP/IP

Les données sont **découpées en paquets** de bits. Des machines appelées **routeurs** guident ces paquets à travers le réseau jusqu'à leur destinataire où ils sont réassemblés. Un routeur échange en permanence avec ses voisins pour établir une **carte locale** de ce qu'il voit du réseau. Chaque paquet transite par une série de routeurs, chacun l'envoyant à un autre routeur selon sa carte locale et la destination prévue. Les routeurs s'ajustent en permanence et de proche en proche quand on les ajoute au réseau ou quand un routeur voisin disparaît. Il n'y a plus besoin de carte globale, ce qui permet le routage à grande échelle.

Lors du routage, un paquet peut ne pas arriver pour deux raisons : une panne matérielle d'une ligne ou d'un routeur, ou sa destruction. Chaque paquet contient l'information d'un nombre maximal de routeurs à traverser : pour ne pas encombrer le réseau, il est détruit si ce nombre est atteint. C'est le **protocole TCP** qui fiabilise la communication en redemandant les paquets manquants. Il garantit que tout paquet finira par arriver, sauf panne matérielle incontournable. TCP réordonne aussi les paquets arrivés dans le désordre et diminue la congestion du réseau en gérant au mieux les redemandes.

Le **protocole IP** (*Internet Protocol*), permet d'identifier et de nommer de façon uniforme tous les ordinateurs ou objets qui sont connectés.

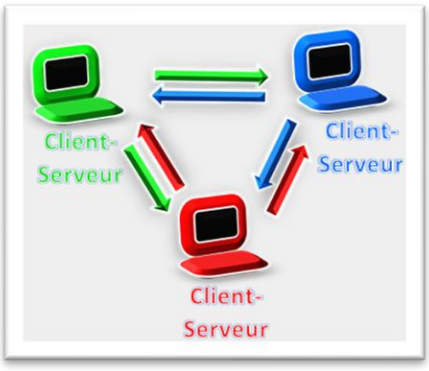
3. L'annuaire d'internet (DNS : Domain Name System)

On associe aux adresses IP des **adresses symboliques** qui sont de courts textes plus simples à retenir. La correspondance entre adresse IP et adresse symbolique est réalisée par **l'annuaire DNS**.

L'annuaire DNS est réparti sur un grand nombre d'ordinateurs répartis sur le réseau et constamment mis à jour.

4. Le modèle pair à pair (peer-to-peer)

Les ordinateurs d'un réseau peer-to-peer sont à la fois client et serveur et peuvent donc tous demander ou envoyer des informations. Ceci accélère les échanges de données et évite l'engorgement du réseau. Il permet à des ordinateurs en réseau d'échanger des fichiers par blocs. Ils peuvent à la fois les recevoir ou les émettre.



5. Impacts sur les pratiques humaines

Mini-Projet : Créer une affiche afin de mettre en garde contre des problèmes ou des dangers d'Internet, à rendre au format .odt ou .docx sur Pronote (elles seront imprimées au format A3).

Idées de recherche : neutralité du Net remise en cause, coût et impact écologique du trafic, « Cliquer c'est polluer ! », différents types de cyberattaques, virus, piratage, hacker, phishing, ransomware, malware, attaque par déni de service, attaque man-in-the-middle, tunneling DNS ...