Comment fonctionne l’internet dans les coulisses

Prénom : Guilherme

Nom : Gaspar Carvalho

Classe : 4C5

Maison : Schoenfels

Tuteur : Jean Majerus

2025-2026

Table de matières

1. Introduction 2
   1.1. Pourquoi ai-je choisi ce sujet 2
   1.2. Objectifs du projet 2
   1.3. Questions principales 3
2. L'histoire et l'évolution d'Internet 3
   2.1. Les origines : ARPANET et les premiers réseaux 3
   2.2. La naissance du World Wide Web 4
   2.3. L'évolution vers l'Internet moderne (fibre, Wi-Fi, 5G...) 5
3. Les bases techniques d'Internet 6
   3.1. Les ordinateurs et les serveurs 6
   3.2. Les routeurs et les câbles sous-marins et les communications par satellites 8
   3.3. Les protocoles : TCP/IP, DNS, HTTP 10
   3.4. Architecture et fonctionnement des réseaux 11
   3.5. Infrastructure et distribution d'Internet 13
4. Le voyage d'une donnée 13
   4.1. Que se passe-t-il quand on tape une adresse dans un navigateur ? 14
   4.2. Le rôle des DNS (trouver le bon serveur) 14
   4.3. Le transfert des paquets de données 15
5. Les sites web et les hébergements 16
   5.1. Qu'est-ce qu'un serveur web ? 17
   5.2. Comment les développeurs mettent un site en ligne 17
   5.3. Les centres de données et le cloud 20
   5.4. Virtualisation, conteneurs et répartition de charge (Cloud moderne) 21
6. La sécurité sur Internet 22
   6.1. Le cryptage et les certificats HTTPS 22
   6.2. Les pares-feux et la protection des données 23

6.3. Les menaces courantes (virus, piratage, phishing) 24
6.4. Risques et protection sur Internet 25
7. L'impact d'Internet sur la société 26
7.1. Communication, travail, et éducation 26
7.2. Les inégalités d'accès à Internet (fracture numérique) 27
7.3. L'avenir du réseau (Internet des objets, satellites, IA...) 28
7.4. Les évolutions des réseaux de communication du futur 30
7.4.1. Les constellations de satellites (Starlink, OneWeb...) 30
7.4.2. Internet plus résilient : multi-chemins, satellites + fibre + 5G 30
7.4.3. Rôle futur de l'IA dans la gestion du réseau 30
8. Conclusion 31
8.1. Ce que j'ai appris 31
8.2. Pourquoi comprendre Internet est important pour un futur développeur 31
8.3. Réflexion personnelle 32
9. Sources 32

1. Introduction

1.1. Pourquoi ai-je choisi ce sujet

Il y a plusieurs raisons pourquoi j'ai choisi ce projet. La première est que pour un carrier de développeur, il est très important de comprendre comment Internet fonctionne et tous les choses qui se déroulent mais qu'on ne voit pas et donc pour mieux comprendre, j'ai décidé d'effectuer quelques recherches sur ce sujet et plus tard j'ai décidé d'écrire un Trape sur ce sujet-là pour mieux comprendre le sujet et pour possiblement enseigner ces mêmes choses que j'ai appris aux gens qui liraient ce Trape. Une autre raison pourquoi j'ai choisi ce sujet était par pur intérêt. Il y a plein d'outils et de technologies qui facilitent l'utilisation d'Internet et la navigation mais il y a plein de choses qui se passent derrières nos écrans dont nous avons aucune idée qui se passent et donc après avoir pensé à ce fait, je me suis rapidement intéressé sur ce sujet et j'ai donc décidé de faire un Trape sur ce thème.

1.2. Objectifs du projet

L'objectif principale de ce projet est de m'apprendre quelques informations importantes que j'aurais besoin si je choisi suivre un carrier de développeur. Je ne voulais pas juste apprendre quelques faits intéressants d'Internet mais je les voulais aussi apprendre car ils seront très utiles pour ma vie professionnelle mais aussi pour ma vie quotidienne.

1.3. Questions principales

Avec ce projet, je voudrais aussi répondre à quelques questions principales. Ces questions seraient donc :

- Comment les données circulent sur Internet ?
- Qu'est-ce qu'un serveur ?
- Comment les sites web deviennent accessibles à tous ?

Après terminer ce travail, j'espère être capable de répondre à ces questions.

2. L’histoire et l’évolution d’Internet

2.1. Les origines : ARPANET et les premiers réseaux

ARPANET (Advanced Research Projects Agency Network) est l’ancêtre internet. Ce projet fut lancé en 1966, mais ARPANET ne voit le jour qu'en 1969. Sa première démonstration officielle date d'octobre 1972.

Arpanet a été créé par le ministère américain de la défense (DARPA) avec le but de connecter des centres de recherche militaires et universitaires, permettant le partage de ressources informatiques et la communication résiliente grâce à la communication par paquets, conçue pour survivre à une attaque nucléaire en redirigeant les données

La communication par paquets est une méthode de réseau qui divise les données en petits blocs appelés paquets, chacun marqué avec des informations d’origine et de destination. Ces paquets sont ensuite envoyés indépendamment sur des chemins optimaux. Arrivé dans leur destination, ces paquets sont donc réassemblés. Cette méthode optimise l’utilisation des ressources réseau et la vitesse. La communication par paquets constitue donc le fondement de l’internet

Avec l’arrivé d’ARPANET, plusieurs innovations ont été introduit au monde. Commençons avec le plus important, la communication par paquets, qui a permis que la communication entre ordinateurs distants soit possible. L’ARPANET a aussi introduit l’envoi de courriels (également connu sous le nom “email”) mais aussi les bases des protocoles de communication. Sans ces protocoles de communication, la communication entre des appareils différents ne serait pas possible. Les premiers protocoles étaient le “TCP” et le “IP”.

Arpanet était un élément fondamental de l'internet d'aujourd'hui. ARPANET s’est développé au fil du temps et autres réseaux ont été créés. Dans les années 1980, l’adoption du protocole TCP/IP a permis d’interconnecter différents réseaux entre eux. Grâce à cette interconnexion, Internet tel que nous le connaissons aujourd’hui a vu le jour.

2.2. La naissance du World Wide Web

Le World Wide Web (ou WWW) est un système de gestion d'informations décentralisé qui fonctionne sur l'internet. Ce n'est pas un seul endroit qui contrôle tout. Les informations sont réparties entre plusieurs ordinateurs ou serveurs, et pas dans un seul centre. Ce système a été inventé par Tim Berners-Lee en 1989-1990 au CERN (Organisation européenne pour la recherche nucléaire). Le CERN est le plus grand laboratoire de physique des particules au monde. Le WWW a été inventé avec le but de faciliter le partage et l'accès aux informations entre chercheurs et ordinateurs dans le monde.

Le fonctionnement du système WWW est très facile à comprendre. Les informations sont stockées sur des serveurs web. Chaque page a une adresse appelé URL (par exemple : https://www.example.com). Un navigateur comme Google Chrome, Mozilla Firefox ou Safari permet d'ouvrir ces pages. Finalement, les pages sont reliées entre elles par des liens hypertextes, ce qui permet de naviguer d'une page à l'autre.

La différence entre Internet et le Web n'est peut-être pas si évidente au premier abord, mais il existe une différence cruciale entre les deux. L'internet est un grand réseau mondial d'ordinateurs connectés entre eux qui permet aux ordinateurs de communiquer et d'échanger des données entre eux. Alors que Le World Wide Web est un système de pages web et de sites web reliés par des liens (hyperliens). On y accède avec un navigateur comme Google Chrome ou Mozilla Firefox. Pour mieux comprendre, l'internet est comme les routes qui relient les villes alors que le WWW est les maisons et les magasins que l'on visite grâce à ces routes.

Après sa création, le WWW s'est développé très rapidement grâce à plusieurs étapes importantes. En 1993, le CERN a décidé de rendre le Web libre et gratuit, ce qui a permis à tout le monde de l'utiliser et de créer des sites. Peu après, Des navigateurs ont été créés pour faciliter l'accès aux pages web, cela a rendu le Web plus facile à utiliser pour le grand public. Plus tard, dans les années 2000's de plus en plus d'entreprises et de particuliers créent des sites. Dans cette époque, les moteurs de recherche comme google apparaissent. Tout cela permet aux internautes de trouver des informations plus facilement. À cette même époque, le Web 2.0 est apparu, ce qui a permet aux utilisateurs de pas seulement lire les pages mais aussi de publier du contenu. Aujourd'hui, le WWW est encore en train de se développer et d'évoluer.

Le WWW a révolutionné la société en démocratisant l'accès à l'information, transformant radicalement la communication, le commerce et l'éducation.

La naissance du World Wide Web est un moment clé dans l'histoire de l'internet parce qu'elle a transformé l'internet en un outil simple, accessible et utilisé par des milliards de personnes dans le monde.

2.3. L’évolution vers l’Internet moderne (fibre, Wi-Fi, 5G…)

La fibre optique est un câble très fin fait de verre ou de plastique qui sert à transmettre des informations sous forme de lumière. Elle est utilisée pour fournir Internet très rapide, mais aussi pour la télévision et les communications téléphoniques. La fibre optique est un fil très fin, plus ou moins si fin qu’un cheveu, composé principalement de verre. Le fonctionnement se déroule te tel façon, les données sont converties en impulsions de lumière. Cette lumière se déplace à l’intérieur de la fibre en se réfléchissant sur les parois**.** Le signal peut parcourir de très longues distances avec très peu de perte de qualité.

Une autre chose très connue dans le rayon de la technologie aujourd’hui est le Wi-Fi. Le Wi-Fi a joué un rôle important dans l’évolution de la technologie et d’Internet. Le Wi-Fi est une technologie de réseau sans fil basée sur des ondes radio, permettant aux appareils (ordinateurs, smartphones, TV) de se connecter à Internet et d'échanger des données sans câbles. Le Wi-Fi a donc profondément transformé l’accès à Internet en rendant l’accès à l’internet plus flexible, plus mobile et plus universel, ce qui a accéléré son adoption dans la vie quotidienne.

Le 5G est la version plus récente d’une technologie très utilisée de nos jours dont beaucoup la connaissent sous le nom de "réseaux mobiles". Le 5G est une technologie de réseau sans fil qui utilise de nouvelles fréquences et infrastructures pour offrir des vitesses de connexion beaucoup plus élevées, une latence très faible (temps de réponse rapide) et la capacité de connecter beaucoup plus d’appareils en même temps. Et très similaires aux autres technologies, la 5G rend Internet mobile plus rapide, plus réactif et capable de connecter davantage d’appareils, ouvrant la voie à de nouveaux usages technologiques.

Comme déjà mentionné, la fibre optique, le Wi-Fi et la 5G ont amélioré le quotidien en rendant Internet plus rapide, plus accessible et plus pratique. La fibre permet des connexions très rapides à domicile, le Wi-Fi offre une utilisation sans fil, et la 5G assure une connexion en mobilité. Grâce à ces technologies, il est plus facile de travailler, étudier, communiquer et se divertir en ligne, tout en connectant plusieurs appareils en même temps.

Ces évolutions ont transformé Internet en un réseau mondial moderne car il est devenu plus accessible, plus rapide et mieux adapté aux besoins actuels. Il permet aujourd'hui de connecter en permanence les personnes, les appareils et les services à l'échelle mondiale, et de répondre à des usages modernes comme la communication, le travail à distance et le divertissement en ligne.

3. Les bases techniques d'Internet

3.1. Les ordinateurs et les serveurs

Un ordinateur personnel est une machine conçue pour un utilisateur à la fois. On utilise ces machines pour des choses comme la navigation sur Internet, le traitement de texte ou pour regarder des vidéos, jouer, etc. Il est optimisé pour être rapide et confortable à utiliser directement (écran, clavier, souris).

Un serveur est plutôt conçu pour servir d'autres ordinateurs via un réseau. Il sert à héberger des sites web, stocker et partager des fichiers, gérer des bases de données et fournir des services (courriel, applications, etc.). Un serveur est optimisé pour fonctionner tout le temps. Il gère plusieurs utilisateurs en même temps et est plus stable et sécurisé.

Leur différence principale est qu'un ordinateur est un outil pour consommer des services alors qu'un serveur fourni ces services.

Les serveurs sont obligés d'être plus robustes que les ordinateurs classiques parce qu'ils sont au cœur de fonctionnement des services numériques. S'ils tombent en panne, beaucoup d'utilisateurs sont impactés en même temps donc c'est crucial qu'ils restent en fonctionnement à toute heure. Un ordinateur personnel peut être éteint ou redémarré régulièrement, alors qu'un serveur comme ceux de Google ou de Netflix, doivent rester allumé en permanence, sinon leurs services deviennent inaccessibles. Une autre raison fondamentale, pour quoi les serveurs doivent être plus robustes, est qu'un serveur traite parfois des milliers ou millions de requêtes en même temps, il doit donc supporter une forte charge et éviter les ralentissements. Leur sécurité est aussi fort obligée d'être très renforcé car les serveurs stockent souvent des données personnelles et des informations sensibles qui doivent être mieux protégées contre les piratages, les pertes de données et les attaques informatiques.

Les serveurs que tu utilises tous les jours ne sont pas "dans Internet" de façon abstraite, ils sont physiquement stockés dans des lieux bien réels. La majorité des serveurs se trouvent dans des bâtiments spécialisés appelés data centers par exemple Google Data Centers ou Amazon Web Services, ce sont deux des serveurs plus connus qui existent dans le monde. Ces serveurs sont répartis dans le monde entier et parfois plus proches de toi que tu penses.

Les ordinateurs communiquent avec les serveurs grâce à un ensemble de règles et de technologies réseau qui permettent d'envoyer et recevoir des données à travers Internet. La communication suit presque toujours le même modèle, ton ordinateur envoie une requête, le serveur la reçoit et la traite et puis il renvoie une réponse. Les ordinateurs utilisent aussi des protocoles pour se comprendre. Ces protocoles définissent comment les données sont envoyées et structurées.

On utilise plusieurs serveurs pour un même site ou service parce qu'un seul serveur ne roustis suffit généralement pas à garantir performance, fiabilité et disponibilité à grande échelle. On utilise donc plusieurs serveurs pour gérer beaucoup d'utilisateurs simultanément. C'est aussi pratique pour éviter les pannes et pour réduire le temps de réponse. Finalement, on utilise plusieurs serveurs pour faire évoluer le service facilement. En fait, un site moderne est en réalité un réseau de serveurs qui travaillent ensemble, pas une seule machine.

3.2. Les routeurs et les câbles sous-marins et les communications par satellites

Un routeur est un appareil qui permet de diriger les données sur un réseau, notamment entre ton réseau domestique et Internet. Ça peut aussi être un logiciel. Un routeur relie ton réseau d'une maison par exemple ou d'un bureau à l'internet via ton fournisseur (comme Orange ou Post). Il partage la connexion Internet entre plusieurs appareils comme les téléphones, les ordinateur, les tablettes et aussi les télévisions connectées. C'est le routeur qui permet d'avoir du Wi-Fi à la maison. Le routeur décide où envoyer chaque information par exemple, une requête vers google est envoyée sur Internet alors qu'un fichier vers son imprimante est envoyé localement. Le routeur est aussi responsable pour la sécurisation des échanges de données. Il bloque certaines connexions extérieures et agit aussi comme un pare-feu basique. En conclusion, le routeur est comme un chef de circulation pour Internet chez chacun.

Un autre moyen de transmettre des données qui est aussi très essentiel, sont les câbles sous-marins. Câble sous-marin est un câble au fond des océans pour transporter des données entre les continents. Ce sont des long câbles qui relient des pays entre eux sous la mer. À l'intérieur, on trouve de la fibre optique, qui transmet les données sous forme de lumière (grâce au principe de Fibre optique). Internet mondial dépend de ces câbles, environ 95% du trafic Internet international passe par ces câbles. Ces câbles sont en fait les autoroutes invisibles d'Internet, sans eux, le réseau mondial serait lent, instable ou même impossible. Les câbles sous-marins sont essentiels, mais leur fonctionnement pose plusieurs défis comme par exemple, leur installation peut coûter très chère et elle est aussi très complexe, ces câbles sont aussi très fragiles.

Finalement, les satellites de communication. Un satellite de communication est un satellite artificiel conçu pour transmettre des informations (voix, Internet, télévision) entre différents points sur Terre. Aujourd'hui, les satellites sont partout autour de nous et remplissent des fonctions très diverses. Des usages des satellites principaux sont la communication (Télévision - chaines diffusées par satellites, Téléphone et Internet et Radio et réseaux militaires), la navigation et géolocalisation (des choses comme le GPS) ou aussi la sécurité et défense (surveillance militaire et renseignement et détection des missiles et communications sécurisées).

Ces 3 moyens de transmettre des données sont essentiels parce qu'Internet repose sur un réseau mondial physique et logique pour transmettre les données rapidement et de manière fiable. Chacun joue un rôle spécifique. Le routeur est comme le chef de circulation d'Internet chez chacun ou dans un réseau, les câbles sous-marins sont les autoroutes mondiales et les satellites sont la couverture globale. Internet repose sur des infrastructures physiques (câbles, routeurs) et des relais aériens (satellites) pour que les données circulent vite, loin et partout

3.3. Les protocoles : TCP/IP, DNS, HTTP

Un protocole est un ensemble de règles ou de conventions qui définissent comment des éléments communiquent ou interagissent entre eux. C'est un peu comme un langage commun qui permet à différents systèmes ou personnes de se comprendre et de fonctionner correctement ensemble. Ces protocoles sont responsables pour l'organisation de la communication entre ordinateurs ou appareils. Un protocole (en termes d'informatique) est un cadre de règles qui garantit que tout se passe correctement entre plusieurs parties.

Un protocole très important et connu est le HTTP (dans chaque URL, tout au début). HTTP est le langage principalement de communication du web. Le protocole HTTP est essentiel pour afficher une page web parce qu'il permet la communication entre ton navigateur et le serveur où se trouve le site. Un autre protocole très connu est le HTTPS. En fait, ces deux protocoles sont très similaires un à l'autre mais il y a une différence cruciale qui concerne la sécurité des données. Avec le HTTP, les données sont envoyées en clair (sans être protégées ou chiffrées), elles peuvent être interceptées ou modifiées par des personnes malveillantes et utilisées pour des sites non sensibles alors qu'avec le HTTPS, les données sont chiffrées, protégées contre l'interception et elles utilisent un certificat de sécurité comme SSL ou TLS. Ces certificats sont des fichiers installés sur un site web qui permettent de vérifier l'identité du site et que permettent de chiffrer les données.

Les protocoles comme HTTP, HTTPS et TCP/IP travaillent ensemble en couches pour permettre le fonctionnement d'Internet. Ensemble, ils permettent d'avoir un web fonctionnel, organisé et sécurisé.

De nos jours, il est très important de comprendre les bases de ces protocoles car ça nous permet de mieux utiliser l'internet, de naviguer de façon plus sécurisée et de développer des compétences utiles en informatique. C'est un peu comme comprendre les règles de la route avant de conduire. Ça rend tout plus clair et plus sûr.

3.4. Architecture et fonctionnement des réseaux

Internet repose sur un ensemble de règles, appelées protocoles, ainsi que sur différentes technologies qui permettent aux appareils (ordinateurs, smartphones, serveurs…) de communiquer entre eux à travers le monde. Sans ces règles communes, les échanges de données seraient impossibles.

Chaque appareil connecté à Internet possède une adresse IP, qui est un identifiant unique permettant de le reconnaître sur le réseau. On peut comparer cette adresse à une adresse postale : elle indique où envoyer les informations. Il existe deux versions principales : IPv4, encore largement utilisée aujourd'hui, et IPv6, plus récente, qui permet de créer un nombre beaucoup plus important d'adresses pour répondre à la croissance d'Internet.

En plus de l'adresse IP, les ports jouent un rôle essentiel. Ils permettent de diriger les données vers le bon service sur un appareil. Par exemple, un ordinateur peut recevoir en même temps des données pour un site web et pour un courriel, chacun passant par un port différent. Les protocoles TCP et UDP définissent la manière dont ces données sont envoyées : TCP garantit une transmission fiable et ordonnée, tandis que UDP privilégie la rapidité, quitte à perdre certaines informations.

Enfin, le fonctionnement d'Internet peut être mieux compris grâce au modèle OSI, qui découpe la communication en 7 couches. Chaque couche a une fonction spécifique, allant de la transmission physique des données jusqu'à leur affichage à l'écran. Ce modèle permet d'organiser et de simplifier les échanges, en rendant plus clair le rôle de chaque étape dans la communication entre deux appareils.

3.5. Infrastructure et distribution d'Internet

Internet ne correspond pas à un seul réseau centralisé, mais à une immense infrastructure composée de millions de réseaux interconnectés à travers le monde. Ces réseaux appartiennent à différentes organisations : entreprises, universités, gouvernements ou encore fournisseurs d'accès. Leur interconnexion permet aux utilisateurs de communiquer et d'accéder à des ressources situées n'importe où sur la planète.

Les utilisateurs accèdent à Internet grâce aux fournisseurs d'accès à Internet (FAI). Ces entreprises fournissent une connexion via des technologies comme la fibre optique, l'ADSL ou la 4G/5G. À domicile, la box Internet joue un rôle essentiel : elle relie les appareils (ordinateurs, smartphones, objets connectés) au réseau du FAI et gère la distribution de la connexion au sein du réseau local.

Une fois connecté, les données doivent souvent traverser plusieurs réseaux avant d'atteindre leur destination. Pour organiser ces échanges à grande échelle, Internet utilise des protocoles de routage comme le BGP (Border Gateway Protocol). Ce protocole permet aux différents réseaux de communiquer entre eux et de choisir les meilleurs chemins pour faire circuler les données, en tenant compte de critères comme la rapidité ou la disponibilité des routes.

Enfin, pour améliorer les performances et réduire les temps de chargement, des systèmes appelés CDN (Content Delivery Networks) sont largement utilisés. Ces réseaux de distribution de contenu reposent sur des serveurs répartis dans différentes régions du monde. Ils stockent des copies de données populaires (sites web, vidéos, images…), ce qui permet aux utilisateurs d'y accéder depuis un serveur proche géographiquement. Cela réduit la latence, diminue la charge sur les serveurs principaux et améliore l'expérience globale des utilisateurs.

4. Le voyage d'une donnée

4.1. Que se passe-t-il quand on tape une adresse dans un navigateur ?

Le navigateur ne comprend pas les noms comme google.com, il a besoin d'une adresse IP (comme 142.250.74.14). Un DNS (Domain Name System) est donc utilisé pour traduire le nom d'une site web en adresse IP. Une fois l'adresse IP obtenu, le navigateur ouvre une connexion vers cette IP. Il utilise généralement le protocole HTTP ou HTTPS (sécurisé). Puis le serveur renvoie du code HTML (structure de la page), du CSS (design) et du Javascript (interactions).

Quand le navigateur reçoit la réponse du serveur, il commence par analyser le HTML pour construire une structure appelée DOM, qui représente tous les éléments de la page. Ensuite, il charge les fichiers CSS afin de déterminer le style de chaque élément, puis combine structure et styles pour créer ce qui doit être affiché à l'écran. Il calcule alors la position et la taille de chaque élément (mise en page), avant de les dessiner visuellement (affichage). Enfin, le JavaScript peut modifier la page en temps réel, ce qui peut entraîner de nouveaux calculs et mises à jour de l'affichage.

Si quelque chose ne fonctionne pas, le navigateur essaie quand même d'afficher la page, mais il peut montrer des erreurs. Par exemple, si le serveur ne trouve pas la page, il renvoie une erreur comme 404, ou s'il y a un problème interne, une erreur 500. Si le réseau ne fonctionne pas, la page ne se charge pas du tout. Des erreurs dans le code peuvent aussi provoquer un affichage incomplet ou des fonctionnalités qui ne marchent pas. Dans tous les cas, le navigateur affiche soit un message d'erreur, soit une version partielle de la page.

4.2. Le rôle des DNS (trouver le bon serveur)

Un DNS (Domain Name System) est comme un annuaire d'Internet. Il sert à traduire les noms de sites web faciles à lire (comme google.com) en adresses IP numériques (comme 142.250.74.14) que les ordinateurs utilisent pour communiquer. Donc quand tu tapes une adresse dans ton navigateur, ton ordinateur ne comprend pas directement ce nom. Il a besoin de connaître l'adresse IP du serveur qui héberge le site. Le DNS fait donc le lien entre le nom du domaine et l'adresse IP.

Le DNS aide à trouver le bon serveur en traduisant le nom de domaine qu'un utilisateur saisit (comme un site web) en une adresse IP unique correspondant au serveur qui héberge ce site. Lorsqu'une requête est envoyée, le DNS interroge plusieurs serveurs de manière hiérarchique jusqu'à obtenir l'adresse IP exacte. Une fois cette information trouvée, elle est renvoyée à l'ordinateur de l'utilisateur, qui peut alors se connecter directement au bon serveur pour afficher le contenu demandé.

Il existe quatre principaux types de DNS : le DNS récursif, qui reçoit la demande de l'utilisateur ; les serveurs racine, qui orientent la recherche ; les serveurs TLD, qui gèrent les extensions comme .com ; et les serveurs autoritaires, qui donnent l'adresse IP finale du site.

Si le DNS ne fonctionne pas, ton ordinateur ne peut plus traduire les noms de domaine en adresses IP, ce qui empêche d'accéder aux sites web en utilisant leur nom habituel. Même si la connexion Internet est active, le navigateur ne parvient pas à trouver le serveur correspondant et affiche une erreur. En conséquence, la navigation devient très limitée, voire impossible sans connaître directement les adresses IP des sites.

Le DNS est donc un chose très crucial pour Internet car elle permet de relier les noms de domaines aux adresses et pour cette raison, rend la navigation simple et rapide pour les utilisateurs. Le DNS permet de trouver le bon serveur parmi des millions. Sans DNS, Internet serait très difficile à utiliser.

Les DNS peuvent être utilisés pour la sécurité en bloquant l'accès à des sites dangereux, en filtrant certains contenus et en aidant à détecter des activités suspectes comme le phishing ou les attaques malveillantes.

4.3. Le transfert des paquets de données

Un paquet de données est une unité de base utilisée pour transmettre des informations sur un réseau informatique, comme Internet. Plutôt que d'envoyer un fichier ou un message entier d'un seul coup, les ordinateurs le découpent en petits morceaux (les paquets) pour que la transmission soit plus rapide et fiable. Un paquet contient généralement les données utiles qui est la partie réelle de l'information que vous voulez envoyer (texte, image, vidéo, etc.) et des informations de contrôle, par exemple l'adresse de l'expéditeur et du destinataire, l'ordre des paquets, et des codes pour vérifier l'intégrité des données.

Chaque paquet peut voyager indépendamment des autres et peut emprunter différents chemins dans le réseau. À l'arrivée, les paquets sont réassemblés pour reconstituer le fichier ou le message complet.

Pour reconstituer correctement les données à partir des paquets, les ordinateurs utilisent plusieurs mécanismes. Au début, chaque paquet reçoit un numéro d'ordre avant d'être envoyé pour que même si les paquets arrivent dans le désordre, l'ordinateur sait comment les remettre dans le bon ordre grâce à ces numéros. Puis, l'ordinateur détecte si le paquet a été endommagé pendant le transport ou si un paquet est corrompu, si c'est le cas, l'ordinateur demande simplement qu'il soit renvoyé, plutôt que de rejeter tout le fichier. Une fois tous les paquets reçus, l'ordinateur les range dans l'ordre grâce aux numéros. Il vérifie l'intégrité de chaque paquet avec les codes de contrôle et finalement, l'ordinateur recombine les données pour former le fichier ou le message original.

Tout ce processus est géré par des protocoles réseau comme TCP (Transmission Control Protocol) car il garantit que les paquets arrivent complets et dans le bon ordre et UDP (User Datagram Protocol) car il envoie les paquets rapidement mais sans garantie de réassemblage (utile pour le streaming ou les jeux en ligne où la vitesse compte plus que la perfection).

Les données sont envoyées en paquets, petits morceaux numérotés et vérifiés, plutôt qu'en une fois car cela permet de les transmettre plus vite, de corriger les erreurs facilement, et de les reconstituer correctement à l'arrivée.

Le transfert des paquets peut être affecté par plusieurs problèmes qui ralentissent ou perturbent la communication. Les principaux sont des problèmes comme la perte de paquets, des paquets qui peuvent arriver en retard ou désordonnés, la corruption des paquets et la congestion du réseau.

5. Les sites web et les hébergements

5.1. Qu'est-ce qu'un serveur web ?

Un serveur web est un logiciel (et parfois aussi la machine physique sur laquelle il tourne) qui permet de stocker, traiter et envoyer des pages web aux utilisateurs via Internet. Son rôle principal est d'héberger des sites web, répondre aux requêtes des utilisateurs, fournir le contenu (pages, fichiers, données) et gérer les connexions entre les utilisateurs et le site.

Un serveur web fonctionne grâce à un échange entre un navigateur et un serveur. Quand un utilisateur entre une adresse, le navigateur envoie une requête HTTP. Le serveur, via des logiciels comme Apache HTTP Server ou Nginx, traite cette demande et renvoie une réponse contenant la page ou les données demandées. Le navigateur affiche ensuite le contenu à l'écran.

Un serveur web peut gérer différents types de contenus, selon les besoins du site. Ces contenus peuvent être des fichiers statiques (pages HTML, fichiers CSS, Images (JPEG, PNG) ou des vidéos ou fichiers audio), du contenu dynamique, ce sont des contenus générés à la demande comme pages personnalisées (par exemple un profil utilisateur), résultats de recherche et données issues d'une base de données mais aussi d'autres types de contenu comme des fichiers à télécharger (PDF, ZIP) ou des applications web complètes.

Il y a deux types de serveurs, les serveurs physiques et les serveurs cloud. Leurs différences principales sont que les serveurs physiques sont locaux et matériels, tandis que les serveurs cloud sont virtuelles, ce que les rends plus flexibles et accessibles en ligne.

Un serveur web assure la sécurité d'un site grâce à plusieurs mécanismes qui protègent les données et les utilisateurs. Les serveurs web protègent donc les sites en chiffrant les données, contrôlant les accès et en bloquant les attaques, tout ça en restant à jour.

5.2. Comment les développeurs mettent un site en ligne

Avant qu'un texte puisse être mis en ligne pour un accès public global, il faut que le, respectivement les développeurs s'assurent qu'il n'y ait plus de fautes d'orthographe dans leurs textes si présents, ou que toutes les images soient bien appropriées au sujet de leur site. Il faut aussi s'assurer que toutes les informations et pages importantes soient présentes sur le site, ou en rajouter s'il en manque. Le/les développeurs doivent aussi s'assurer que tous les liens fonctionnent encore ou qu'ils n'aient pas mal copie un lien. Si le site contient des fonctionnalités spéciales, par exemple une barre de recherche intégrée ou un système de paiement, il faudrait aussi s'assurer que tous ces systèmes fonctionnent comme ils devraient. Pour une expérience plus accommodée de l'utilisateur, le développeur devrait aussi s'arranger pour que le site fonctionne aussi rapidement et facilement que possible. Pour cela il est indispensable que le site fonctionne parfaitement sur tous les appareils, par exemple tablette ou portable. Pour la meilleure des expériences un développeur devrait aussi tester son site sur plusieurs navigateurs, c'est-à-dire google ou Firefox. Pour le design du site il y a beaucoup de possibilités, par exemple le développeur peut s'arranger pour que les URLs soient aussi courtes que possibles et ne prennent pas trop de place, il peut aussi structurer son site avec des titres ou des balises. Il est aussi indispensable de sécuriser son site avec des anti-bot CAPTCHA et des anti-spams, et surtout de sauvegarder le site afin de jamais y perdre accès. Une des étapes les plus importantes pour la finalisation et publication d'un site est de se rendre sur que le site est bien légal, c'est-à-dire qu'il faut ajouter une bannière de cookies, et aussi mettre des mentionnes légales pour les images par exemple. Avant la publication du site, il faut encore ajouter le domaine du site et mettre en place les courriels professionnels ou encore vérifier les redirections. Pour garder compte des chiffres et analyses, il faut absolument ajouter un outil d'analyse, qui fonctionne comme un robot qui sauvegardera les données dans une base de données pour que le développeur et l'utilisateur du site puissent regagner accès aux données passées.

Enfin, le site est prêt à être publie, mais même après sa mise en ligne, il reste important de tester le site pour voir s'il fonctionne bien comme entendu et qu'il n'y ait pas de bugs ou d'erreurs qui surviennent. Le développeur peut maintenant être fier : il a maintenant avec succès publie un site. Mais cela ne signifie pas qu'il ne doit pas garder un œil sur son site. Pour une expérience aussi complète que possible, il faudrait régulièrement mettre à jour le contenu du site et corriger les bugs qu'il n'aurait pas remarque avant la publication. Si cela est d'intérêt, le développeur devrait aussi surveiller la performance de son site pour voir ce qui rapporte le plus de vues ou d'argent par exemple et peut-être refaire un autre site encore meilleur dans le futur.

Le nom de domaine d'un site est important afin de ne pas avoir à retenir une adresse IP compliquée pour pouvoir accéder à un site, mais juste un nom de préférence mémorable. Le nom de domaine donne aussi un aspect beaucoup plus professionnel au site et on peut l'attacher à des domaines additionnels. Cela sert aussi à garder accès à son propre site et à construire sa présence en ligne. Pour transférer les fiches de son site vers un serveur, il faut d'abord comprendre ce qu'on compte transférer, comme des images ou des fichiers et même des bases de données. Lorsqu'on obtient accès à son outil pour Transfer de fichiers, il faudra le renseigner de toutes ses informations comme son nom d'utilisateur et son mot de passe. Il faudra glisser les fichiers que l'on veut transférer au serveur sur le serveur-même et ensuite s'assurer une dernière fois que tout fonctionne parfaitement et que tout est à sa place. Pour finir il faut aussi encore ajouter une base de données si nécessaire. Un CL/CD sert à envoyer toute mise à jour, y compris une mise à jour directement vers un dépôt et de vérifier automatiquement s'il n'y a pas de bugs ou d'erreurs qui surviennent. Le site est alors directement envoyé et mis à jour sur le serveur sans besoin d'intervention manuelle et le développeur aura ainsi gagne du temps. Le CL/CD est souvent utilise car il est utile pour le travail sur un site commun d'une équipe et car il permet d'éviter l'erreur humaine ou encore de gagner du temps.

5.3. Les centres de données et le cloud

Un centre de données (ou data center) est un site physique qui regroupe des serveurs informatiques, des systèmes de stockage et des équipements réseau permettant de faire fonctionner des services numériques. Presque tout ce qu'on utilise sur Internet tourne grâce à un centre de données. Quelques exemples seraient les sites web, les réseaux sociaux, les services cloud, le streaming vidéo, les applications mobiles et il y en a encore beaucoup d'autres choses. Ces data centers sont essentiels pour le fonctionnement to tous ces choses car ils garantissent que les services numériques sont disponibles 24h/24, rapides, sécurisés et aussi très important, capables de gérer des millions d'utilisateurs en même temps.

Une chose que beaucoup confondent avec un serveur est le cloud. Le cloud désigne le fait d'utiliser des ressources informatiques via Internet, au lieu de les avoir sur ton propre appareil. Le cloud n'est pas un serveur mais ça fonctionne plutôt grâce à ces serveurs. Le cloud, comme un système de stockage mais aussi plein d'autres services, permet donc d'accéder à du stockage, de fournir des logiciels, de la puissance de calcul, des serveurs et aussi du streaming et des jeux en lignes.

Le fonctionnement se déroule de tel façon, quand on fait une action comme ouvrir un fichier sur google drive ou regarder un vidéo sur Netflix, ton appareil envoie une demande via internet, puis cette demande arrive dans un data center. Dans le data center, les serveurs stockent les données, ils les traitent (ouvrir un fichier, lancer un vidéo) et finalement calculent si nécessaire (IA, jeux, etc.). Finalement, le résultat revient vers l'utilisateur. Les données sont donc renvoyées sur leur téléphone, leur tablette ou leur ordinateur et tout cela se fait en quelques millisecondes

Ce qui rend le cloud efficace est que des milliers de serveurs travaillent ensemble, pour une bonne sécurité, les données sont souvent dupliquées et les centres de données sont aussi répartis dans le monde entier pour une rapidité de transmission de données plus élevé.

5.4. Virtualisation, conteneurs et répartition de charge (Cloud moderne)

Le cloud computing moderne repose sur des technologies avancées qui permettent de fournir des services informatiques à grande échelle, tout en optimisant l'utilisation des ressources. L'une des technologies fondamentales est la virtualisation. Elle consiste à créer plusieurs machines virtuelles sur un seul serveur physique. Chaque machine virtuelle fonctionne comme un ordinateur indépendant avec son propre système d'exploitation et ses propres applications. Cela permet aux entreprises d'utiliser un seul serveur pour plusieurs usages différents, ce qui réduit les coûts, améliore la flexibilité et facilite la maintenance des systèmes.

Une évolution plus récente de cette technologie est celle des conteneurs. Contrairement aux machines virtuelles, les conteneurs ne reproduisent pas un système d'exploitation complet. Ils partagent celui de la machine hôte, mais isolent les applications et leurs dépendances dans un environnement fermé. Cela les rend beaucoup plus légers et rapides à démarrer. Les conteneurs sont très utilisés dans le développement moderne d'applications, car ils permettent de déployer facilement un logiciel sur différents environnements sans problème de compatibilité. Des outils comme Docker ou Kubernetes permettent de gérer et d'orchestrer ces conteneurs à grande échelle.

Enfin, la répartition de charge (load balancing) joue un rôle essentiel dans les infrastructures cloud. Elle consiste à distribuer intelligemment les requêtes des utilisateurs entre plusieurs serveurs afin d'éviter qu'un seul ne soit surchargé. Cela permet d'améliorer les performances, de réduire les temps de réponse et d'assurer une meilleure stabilité des services. En cas de panne d'un serveur, le système de répartition de charge redirige automatiquement les requêtes vers d'autres serveurs encore disponibles, garantissant ainsi une continuité du service et une meilleure fiabilité globale.

6. La sécurité sur Internet

6.1. Le cryptage et les certificats HTTPS

Le cryptage est un nom très connu dans la branche d'Internet. Mais c'est aussi une chose très importante et essentiel sur Internet pour plusieurs raisons fondamentales liées principalement à la sécurité et à la confiance. Le cryptage sert à protéger les données sensibles comme des mots de passe, numéros de cartes bancaire, des messages, etc. Le cryptage garantit la confidentialité, il évite aussi les piratages et fraudes et assure aussi l'intégrité des données. En conclusion, le cryptage est principalement responsable de créer un Internet de confiance.

Comme déjà mentionné, le HTTPS est un protocole qui permet principalement de sécuriser la communication. Ce protocole utilise un système de chiffrement qui fonctionne de tel façon, quena le navigateur contacte un site, le site envoie un certificat de sécurité. Puis une connexion chiffrée est établie pour que toutes les données échangées deviennent illisibles pour un tiers. Tout ce processus de cryptage est très important pour que les données des utilisateurs soient protégées et que personne ne puisse espionner facilement. Avec HTTPS, on est sûr d'être sur le bon site.

Pour utiliser HTTPS, il faut obtenir un certificat auprès d'une autorité comme Let's Encrypt. On génère une clé et une demande de certificat, puis on prouve que l'on possède le site. Une fois le certificat installé, les échanges sont sécurisés et doivent être renouvelés régulièrement.

Les navigateurs affichent des alertes pour les sites qui n'utilisent pas HTTPS afin de protéger les utilisateurs. Sans chiffrement, les informations échangées peuvent être facilement interceptées ou modifiées par des personnes malveillantes, notamment sur des réseaux publics. Ces avertissements permettent donc de signaler un risque pour la confidentialité des données et d'encourager l'utilisation de connexions sécurisées.

6.2. Les pares-feux et la protection des données

Un pare-feu (ou *firewall* en anglais) est un outil de sécurité informatique qui sert à contrôler les communications entre ton appareil (ordinateur, téléphone, réseau) et Internet. Sa tâche principale est de protéger ton système contre les accès non autorisés. Objectivement, le pare-feu filtre les données qui peuvent entrer et sortir selon des règles définies, il bloque aussi des connexions suspectes comme un hacker qui tente d'accéder à ton ordinateur et finalement, il empêche certains programmes de communiquer avec Internet.

Pour savoir quels sont les accès et connexions autorisés, le pare-feu analyse chaque connexion et puis il compare ce qu'il a analysé à une liste de règles pour savoir s'il doit bloquer ces connexions ou les autoriser. Finalement, après avoir analysé et comparé, le pare-feu laisse passer ou refuse les connexions.

Il y a deux types de pares-feux qui sont très similaires mais ont quand même quelques différences mineures. Ce sont les pares-feux matériels et logiciel. Les deux ont le même rôle mais leurs différences principales tiennent surtout à où ils sont installés et comment ils protègent. Un pare-feu matériel protège tout un réseau donc tous les appareils connectés. Il est placé entre Internet et un réseau et il fonctionne sans dépendre d'un ordinateur. Un pare-feu logiciel protège plutôt un seul appareil. Il fonctionne directement sur le système (Windows, macOS, etc.) et il peut analyser les applications individuellement. Le meilleur niveau de sécurité est donc de combiner les deux car le pare-feu matériel peut bloquer les menaces globales alors que le pare-feu logiciel contrôle ce qui se passe sur chaque appareil.

Un pare-feu est une protection importante, mais il ne suffit pas à lui seul. Il doit être complété par un antivirus, des mises à jour régulières et des mots de passe forts avec authentification à deux facteurs. La vigilance face aux courriels suspects, l'utilisation de réseaux sécurisés et les sauvegardes régulières permettent aussi de mieux protéger les données. Ensemble, ces mesures assurent une sécurité plus efficace.

Une seule solution ne suffit pas face aux cybermenaces. Cette approche, appelée sécurité en couches, permet de bloquer ou limiter une attaque à différents niveaux. Ainsi, si une protection échoue, les autres prennent le relais, ce qui réduit les risques et protège mieux les données et les systèmes.

6.3. Les menaces courantes (virus, piratage, phishing)

Un virus informatique est un programme malveillant qui s'installe sur un appareil pour perturber son fonctionnement, voler des données ou se copier sur d'autres systèmes. Ces virus peuvent se propager par des fichiers envoyés par courriel ou en ouvrant une pièce jointe qui contient ce virus. On peut aussi attraper un virus en téléchargeant des fichiers depuis des sites non fiables ou le virus peut aussi se cacher dans un programme. Il y a plein de méthodes à comment on peut attraper un virus. Principalement, un virus peut se propager grâce aux actions de l'utilisateur et aux failles de system.

Les virus peuvent causer une grande variété de dégâts. Ils peuvent ralentir ou causer des problèmes de fonctionnements des appareils ou programmes. Ils peuvent aussi supprimer des fichiers importants et corrompre des documents ou faire disparaitre des photos, vidéos ou travaux. Une autre chose qui se répète très souvent est qu'un virus vole des informations personnelles. Et finalement, les virus peuvent aussi se propager à d'autres systèmes. C'est pour cela qu'il est important de se protéger contre ces virus.

Un autre mot très connu dans l'informatique est le piratage informatique. Le piratage informatique est une action illégale qui consiste à accéder sans autorisation à un système, un compte ou un réseau. Les pirates utilisent des failles de sécurité ou des techniques comme le phishing pour voler des données ou tromper les utilisateurs. Leur but est souvent de voler des informations ou d'espionner des personnes.

Le phishing est une technique de fraude utilisée par des pirates pour tromper les utilisateurs afin de voler leurs informations personnelles. Ils envoient souvent des messages (courriels ou SMS) en se faisant passer pour une banque ou un service connu et demandent de cliquer sur un lien ou de donner des données. On peut le reconnaître grâce à des messages suspects, des liens étranges, des fautes d'orthographe ou des demandes urgentes d'informations.

Pour se protéger contre les virus, le piratage et le phishing, il faut adopter de bonnes pratiques de sécurité. Il est important d'utiliser un antivirus et un pare-feu, de mettre régulièrement à jour ses appareils, et de choisir des mots de passe forts et différents pour chaque compte. Il faut aussi éviter de cliquer sur des liens ou de télécharger des fichiers suspects, et vérifier toujours l'authenticité des messages reçus. Enfin, activer la double authentification et faire des sauvegardes régulières permet de mieux protéger ses données.

6.4. Risques et protection sur Internet

Internet est une infrastructure mondiale essentielle, mais elle reste vulnérable à différents types de risques, qu'ils soient techniques ou liés à la sécurité des données. Parmi les menaces les plus fréquentes figurent les attaques DDoS (Distributed Denial of Service). Ces attaques consistent à envoyer un volume massif de requêtes vers un serveur ou un site web afin de saturer ses capacités. Le service devient alors lent, voire totalement inaccessible pour les utilisateurs légitimes. Ce type d'attaque est souvent utilisé pour perturber des entreprises, des institutions ou des plateformes en ligne.

Au-delà des attaques, Internet dépend également d'infrastructures physiques qui peuvent être fragiles. Une grande partie des communications internationales passe par des câbles sous-marins reliant les continents. Une coupure accidentelle ou volontaire de ces câbles peut entraîner des ralentissements importants, voire des interruptions de service dans certaines régions du monde. De même, les data centers, qui hébergent les serveurs et les données, peuvent subir des pannes dues à des problèmes électriques, techniques ou environnementaux. Lorsqu'un grand centre de données tombe en panne, cela peut affecter simultanément de nombreux sites et services en ligne.

En parallèle, la protection de la vie privée est devenue un enjeu majeur à l'ère du numérique. De nombreux sites web utilisent des cookies (petits fichiers stockés sur l'appareil de l'utilisateur) et des trackers pour collecter des informations sur la navigation, comme les pages consultées, le temps passé ou les préférences. Ces données sont souvent utilisées pour personnaliser le contenu ou afficher des publicités ciblées, mais elles soulèvent des questions importantes concernant le respect de la vie privée.

Pour encadrer ces pratiques, des lois comme le RGPD (Règlement Général sur la Protection des Données) ont été mises en place, notamment en Europe. Ce règlement impose aux entreprises de collecter uniquement les données nécessaires, d'informer clairement les utilisateurs sur leur utilisation et d'obtenir leur consentement. Il garantit également aux utilisateurs des droits, comme celui d'accéder à leurs données, de les modifier ou de les supprimer. Ces mesures visent à renforcer la confiance des utilisateurs et à mieux protéger leurs informations personnelles dans un environnement numérique en constante évolution.

7. L’impact d’Internet sur la société

7.1. Communication, travail, et éducation

Internet a transformé la communication en la rendant beaucoup plus rapide, simple et mondiale, car il permet d’échanger instantanément des messages, de passer des appels vidéo et de communiquer avec des personnes partout dans le monde. En même temps, les outils numériques facilitent le travail en permettant de partager des documents, de collaborer en ligne et de travailler à distance grâce à des applications et plateformes. Ainsi, Internet et les technologies numériques ont rendu la communication plus efficace et le travail plus flexible et organisé.

Le télétravail a profondément changé le monde professionnel en permettant aux employés de travailler à distance, sans être obligés de se rendre au bureau. Cela a rendu le travail plus flexible, amélioré parfois l’équilibre entre vie professionnelle et vie personnelle, et réduit les déplacements. Les entreprises utilisent davantage les outils numériques pour communiquer et collaborer en ligne. Cependant, cela peut aussi créer des difficultés comme l’isolement ou une séparation moins claire entre travail et vie privée.

Internet a transformé l’éducation en la rendant plus accessible et plus interactive, car les élèves peuvent désormais apprendre à distance, accéder à une grande quantité de ressources en ligne et suivre des cours depuis n’importe où. Les outils utilisés dans l’enseignement moderne incluent les plateformes de cours en ligne, les visioconférences, les tableaux numériques interactifs et les applications éducatives. Grâce à ces technologies, l’apprentissage est devenu plus flexible, collaboratif et adapté aux besoins des élèves.

Le numérique présente de nombreux avantages dans la vie quotidienne, car il facilite la communication, permet d’accéder rapidement à une grande quantité d’informations et simplifie de nombreuses tâches comme les achats en ligne, les démarches administratives ou le travail à distance. Cependant, il a aussi des limites, comme la dépendance aux écrans, les risques pour la vie privée et la sécurité des données, ainsi que les inégalités d’accès pour certaines personnes.

7.2. Les inégalités d'accès à Internet (fracture numérique)

La fracture numérique désigne les inégalités d'accès et d'usage des technologies numériques (comme Internet, les ordinateurs ou les smartphones) entre différentes personnes ou groupes. En termes plus simples, la fracture numérique est le fait que tout le monde n'a pas les mêmes chances face au numérique, soit à cause du manque d'équipement, soit du manque de compétences. Ce phénomène vient avec quelques effets concrets sur la vie de tous les jours qui peuvent compliquer ou limiter l'accès à des choses essentielles. Cela peut gêner l'éducation car ça peut causer des difficultés à suivre les cours en ligne, la fraction numérique peut aussi mener à moins d'accès aux ressources (vidéos, exercices, recherches). Ce même phénomène peut aussi causer des troubles dans le travail et emploi. On peut rencontrer des difficultés à chercher un emploi car beaucoup d'offres sont en ligne, c'est aussi impossible ou compliqué de faire du télétravail et pour ces raisons-là, on a moins d'opportunités professionnelles. En conclusion, la fracture numérique peut rendre la vie plus difficile, créer des inégalités et isoler certaines personnes dans de nombreux aspects du quotidien.

Certaines zones ont un mauvais accès à Internet à cause de l'éloignement, surtout dans les régions rurales ou isolées, ainsi que du coût élevé des infrastructures qui limite les investissements. De plus, des problèmes techniques comme les zones blanches ou le manque d'électricité peuvent réduire la qualité de la connexion. À l'échelle individuelle, plusieurs facteurs peuvent aussi empêcher une personne d'utiliser Internet, comme le manque d'équipement (ordinateur ou smartphone), le coût de l'abonnement ou encore le manque de compétences numériques. Ainsi, ces difficultés techniques, économiques et sociales contribuent à la fracture numérique.

Les gouvernements et les organisations réduisent la fracture numérique en développant les infrastructures pour améliorer l'accès à Internet, surtout dans les zones rurales. Ils proposent aussi des aides financières pour les équipements et les abonnements, ainsi que des formations pour apprendre à utiliser les outils numériques. Enfin, ils accompagnent les personnes dans leurs démarches en ligne pour rendre les services plus accessibles.

L'accès à Internet est devenu essentiel car il permet de réaliser de nombreuses activités du quotidien. Il est indispensable pour l'éducation, avec les cours en ligne et les recherches, pour le travail, notamment avec le télétravail et la recherche d'emploi, ainsi que pour accéder aux services comme les démarches administratives ou la santé. Internet facilite aussi la communication avec les autres et l'accès à l'information. Sans Internet, il devient donc difficile de participer pleinement à la vie sociale, économique et éducative.

7.3. L’avenir du réseau (Internet des objets, satellites, IA…)

L’Internet des objets (IoT) désigne l’ensemble des objets du quotidien connectés à Internet, capables de collecter et d’échanger des données sans intervention humaine directe. Ces objets, comme les montres connectées, les thermostats intelligents ou encore les voitures modernes, sont équipés de capteurs, de logiciels et de systèmes de communication qui leur permettent de fonctionner de manière autonome et d’interagir entre eux. L’IoT est utilisé dans de nombreux domaines, notamment la maison, la santé, l’industrie et les transports, afin d’améliorer le confort, la sécurité et l’efficacité. Toutefois, son développement soulève aussi des questions importantes liées à la protection des données personnelles et à la sécurité informatique.

Les satellites permettent d’améliorer l’accès à Internet en offrant une connexion dans des zones où les infrastructures terrestres, comme la fibre optique ou les antennes, sont difficiles à installer, notamment dans les régions rurales ou isolées. Grâce aux nouvelles constellations de satellites en orbite basse, comme Starlink développée par SpaceX, la connexion est devenue plus rapide et avec moins de délai qu’auparavant. Cela permet non seulement de connecter davantage de personnes à Internet, mais aussi d’assurer une continuité de service en cas de panne ou de catastrophe. Cependant, certains défis restent présents, comme le coût des équipements, la gestion du grand nombre de satellites et les impacts sur l’environnement spatial.

L’intelligence artificielle (IA) joue un rôle clé dans le futur d’Internet en rendant les services plus intelligents, rapides et personnalisés. Elle permet d’analyser de grandes quantités de données afin de proposer du contenu adapté à chaque utilisateur, comme des recommandations ou des résultats de recherche plus pertinents. L’IA contribue également à améliorer la sécurité en détectant les cybermenaces et les activités suspectes en temps réel. En plus, elle aide à optimiser le fonctionnement des réseaux en gérant le trafic de manière plus efficace. Enfin, elle favorise le développement de nouvelles technologies, tout en soulevant des enjeux importants liés à la vie privée et à l’éthique.

Ces technologies offrent plusieurs avantages pour les entreprises et les particuliers. Pour les entreprises, elles améliorent la productivité, facilitent la prise de décision grâce aux données et permettent de réduire les coûts. Pour les particuliers, elles apportent plus de confort, un meilleur accès à Internet et des services personnalisés. Elles améliorent aussi la sécurité, même si elles posent des questions sur la protection des données.

Le futur réseau Internet doit relever plusieurs défis importants comme la sécurité des données et la protection de la vie privée. Il faut aussi réduire les inégalités d'accès à Internet et mieux gérer l'augmentation du trafic et des objets connectés. Enfin, l'impact environnemental des technologies doit être limité pour un développement plus durable.

L'avenir d'Internet est considéré comme « plus intelligent » car il utilise de plus en plus l'intelligence artificielle pour analyser les données, personnaliser les services et automatiser des tâches. Les objets connectés et les systèmes intelligents permettent aussi de rendre les réseaux plus efficaces et réactifs. Il est vu comme « plus global » parce que les satellites et les nouvelles technologies permettent de connecter des régions du monde qui n'avaient pas encore accès à Internet, réduisant ainsi les inégalités et rendant le réseau accessible presque partout sur la planète.

7.4. Les évolutions des réseaux de communication du futur

7.4.1. Les constellations de satellites (Starlink, OneWeb…)

Les constellations de satellites en orbite basse, telles que celles développées par Starlink ou OneWeb, permettent de fournir un accès Internet global, y compris dans les zones rurales ou isolées. Elles réduisent la dépendance aux infrastructures terrestres et améliorent la couverture mondiale, tout en introduisant de nouveaux défis en termes de gestion du trafic spatial et de latence.

7.4.2. Internet plus résilient : multi-chemins, satellites + fibre + 5G

L'Internet du futur repose sur une architecture multi-chemins, combinant plusieurs technologies (fibre optique, réseaux 5G et satellites). Cette approche permet d'assurer une continuité de service en cas de panne d'un réseau, d'optimiser les performances et d'adapter dynamiquement les flux de données en fonction des conditions du réseau.

7.4.3. Rôle futur de l'IA dans la gestion du réseau

L'intelligence artificielle jouera un rôle central dans la gestion des réseaux de communication. Elle permettra d'optimiser automatiquement le routage des données, de prévoir les congestions, de détecter les anomalies en temps réel et d'améliorer l'efficacité énergétique des infrastructures. L'IA contribuera ainsi à rendre les réseaux plus autonomes, adaptatifs et performants.

8. Conclusion

8.1. Ce que j'ai appris

Ce projet m'as appris beaucoup de choses dont une grande partie est très importante pour comprendre ce qui se passe derrières nos écrans quand on se sert de l'internet. J'ai appris les bases de l'internet donc ce qu'un navigateur devrait savoir pour être capable de naviguer correctement et aussi très important, avec de la sécurité. Puis j'ai aussi appris les choses plus "cachées" et importantes d'Internet comme comment se démarche la communication en générale quand on parle d'Internet comme par exemple comment les serveurs se communiquent entre eux ou comment les données circulent autour du monde et entre les différents outils de navigation et sites web. Et finalement, j'ai aussi effectué des recherches sur l'histoire d'Internet et son impact sur le monde et sur notre société de nos jours.

8.2. Pourquoi comprendre Internet est important pour un futur développeur

Comprendre l'internet est important pour le futur de n'importe-qui. Savoir comment prendre avantage des outils que l'on peut retrouver en ligne peut aider chaque personne à, premièrement, atteindre ses objectifs plus rapidement, sans perdre de temps à prendre des détours inutiles par faute de connaissance de l'internet. Mais aussi, avec les nouvelles générations, on remarque une tendance vers le monde sur l'internet. C'est à dire que, en connaissant comment l'internet fonctionne, les chances de trouver un emploi augmentent significativement, pour tout le monde. En effet, si l'on veut choisir par exemple une vie de développeur pour son futur, il est absolument indispensable de comprendre comment fonctionnent les protocoles HTTP ou les adresses IP, cela rend des processus longs et fatigants comme diagnostiquer les bugs ou optimiser la performance de son site ou application bien plus simple. Un autre facteur qui rend la compréhension de l'internet importante est la sécurité. Non seulement pour l'utilisateur mais aussi pour le développeur, qui préfèrera bien passer une semaine ou deux à mémoriser comment fonctionne l'internet que de produire un site vulnérable. De plus, comprendre le web servira au développeur d'attacher à son site plein d'outils qui peuvent lui faciliter la tâche, ou encore lui servir à collecter des données. Mais le plus important, c'est l'autonomie

8.3. Questions principales (introduction)

- *Comment les données circulent sur Internet ?*

Les données circulent sur Internet sous forme de petits paquets envoyés à travers différents réseaux et reconstitués à leur arrivée grâce à des protocoles comme le TCP/IP. Un serveur est un ordinateur spécialisé qui stocke des informations et les envoie aux utilisateurs lorsqu'ils en font la demande, par exemple lorsqu'on visite un site web. Les sites deviennent accessibles à tous grâce à un ensemble de technologies, notamment les adresses IP et le protocole HTTP, qui permet aux navigateurs de communiquer avec les serveurs et d'afficher les pages web. Ensemble, ces éléments permettent à Internet de fonctionner de manière rapide, fiable et accessible partout dans le monde.

- *Qu'est-ce qu'un serveur ?*

Un serveur est un ordinateur conçu pour stocker, gérer et envoyer des données à d'autres ordinateurs appelés clients. Lorsqu'un utilisateur accède à un site web, son navigateur envoie une requête au serveur, qui répond en fournissant les informations demandées, comme une page web, des images ou des vidéos. Cette communication se fait grâce à des protocoles comme le HTTP, qui permettent un échange clair et structuré entre le client et le serveur. Les serveurs sont essentiels au fonctionnement d'Internet, car ils rendent les contenus disponibles à tout moment.

- *Comment les sites web deviennent accessibles à tous ?*

Les sites web deviennent accessibles à tous grâce à plusieurs éléments techniques qui travaillent ensemble. Chaque site est hébergé sur un serveur et possède une adresse unique appelée adresse IP, mais pour faciliter l'utilisation, on utilise des noms de domaine traduits en adresses IP grâce au système DNS. Ensuite, des protocoles comme le HTTP permettent aux navigateurs de demander et d'afficher les pages web correctement. Grâce à cette organisation, n'importe quel utilisateur peut accéder facilement à un site depuis n'importe où dans le monde.

8.4. Réflexion personnelle

Comme tous les projets dans lesquelles j'ai travaillé ou fait partie, ce projet m'a permis d'acquérir plein de nouvelles informations. Ce projet spécifiquement, m'a enseigné des informations qui pourraient et probablement seront utiles pour moi, comme future développeur mais aussi pour ma vie quotidienne. J'ai trouvé les recherches tel que les résultats très intéressants at la plupart d'eux m'étaient inconnus. Ce projet sera très probablement très important si je choisi suivre une carrière de développeur mais j'ai aussi éprouvé beaucoup de plaisir avec les recherches et à écrire ce projet. Je trouve que cela m'a aussi beaucoup facilité la rédaction de ce projet. J'ai aussi consulté plein de personnes différentes de lieux différents, des enseigneurs de mon école, de spécialistes que j'ai rencontrés dans mon stage et encore beaucoup d'autres personnes qui ont pu m'enseigner quelques choses dont j'avais besoin pour écrire ce Trape. Au contraire, j'ai rencontré quelques difficultés avec certaines étapes de ce projet mais à la fin, j'ai bien réussi à compléter des recherches nécessaires et à bien comprendre ce sujet.

9. Sources

2. L’histoire et l’évolution d’Internet

2.1. Les origines : ARPANET et les premiers réseaux

https://fr.wikipedia.org/wiki/ARPANET

https://fr.wikipedia.org/wiki/Commutation_de_paquets

https://www.opal-rt.com/fr/blogue/communication-protocols-in-embedded-systems/

2.2. La naissance du World Wide Web

https://wire.com/fr/blog/loi-cloud-souverainete-donnees-ue

https://fr.wikipedia.org/wiki/World_Wide_Web

https://home.cern/fr/about/who-we-are

2.3. L’évolution vers l’Internet moderne (fibre, Wi-Fi, 5G…)

https://fr.wikipedia.org/wiki/Fibre_optique

https://fr.wikipedia.org/wiki/Wi-Fi

https://fr.wikipedia.org/wiki/5G

3.Les bases techniques d'Internet

3.1. Les ordinateurs et les serveurs

https://fr.wikipedia.org/wiki/Serveur_informatique

https://www.ovhcloud.com/fr/learn/what-is-cloud-server/

https://servermall.com/fr/blog/serveur-vs-pc-comprendre-les-principales-diff-rences-entre-les-ordinateurs/?srsltid=AfmBOoqWOyvwxMhlBQoNE_UBellRXjb1bdU61NGomTFsRcnMb5oWNc6V

3.2. Les routeurs et les câbles sous-marins et les communications par satellites

https://fr.quora.com/Pourquoi-utilise-t-on-des-c%C3%A2bles-plut%C3%B4t-que-des-satellites-pour-diffuser-internet-dans-le-monde

3.3. Les protocoles : TCP/IP, DNS, HTTP

https://www.cloudflare.com/fr-fr/learning/network-layer/internet-protocol/

https://www.wandesk.fr/protocoles-reseau/

3.4. Architecture et fonctionnement des réseaux

https://sti.ac-versailles.fr/IMG/pdf/reseau.pdf

https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique

3.5. Infrastructure et distribution d'Internet

https://www.ibm.com/fr-fr/think/topics/network-infrastructure

https://fr.wikipedia.org/wiki/Fournisseur_d%27acc%C3%A8s_%C3%A0_Internet

4.Le voyage d’une donnée

4.1. Que se passe-t-il quand on tape une adresse dans un navigateur ?

https://developer.mozilla.org/fr/docs/Web/Performance/Guides/How_browsers_work

https://matthieudesroches.com/articles/quoi-faire-quand-rien-ne-va

4.2. Le rôle des DNS (trouver le bon serveur)

https://fr.wikipedia.org/wiki/Domain_Name_System

https://www.proofpoint.com/fr/threat-reference/dns

4.3. Le transfert des paquets de données

https://fr.wikipedia.org/wiki/Transmission_Control_Protocol

https://fr.wikipedia.org/wiki/Paquet_(r%C3%A9seau)

5.Les sites web et les hébergements

5.1. Qu'est-ce qu'un serveur web ?

https://fr.wikipedia.org/wiki/Serveur_web

https://www.ovhcloud.com/fr/learn/what-is-web-server/

5.2. Comment les développeurs mettent un site en ligne

https://blog-fr.orson.io/creation-de-site-internet/etapes-creation-site-internet

https://www.ovhcloud.com/fr/web-hosting/uc-change-web-hosting/

5.3. Les centres de données et le cloud

https://www.deep.eu/fr/deep-one?gad_source=1&gad_campaignid=23689259672&gbraid=0AAAABC9Rz5rVu8G2kfGIZzrAd2vJ42YUR&gclid=CjwKCAjwnN3OBhA8EiwAfpTYeqHnetWh7izPxPWOmI6ojTxWrzXsA1YZY8yM1QPmEFU7rjPXxvBQ5hoCM7UQAvD_BwE

https://fr.wikipedia.org/wiki/Cloud_computing

https://www.fortinet.com/fr/resources/cyberglossary/data-center

5.4. Virtualisation, conteneurs et répartition de charge (Cloud moderne)

https://www.internet.lu/business/fr/ge/cloud/maintenance.html?gad_source=1&gad_campaignid=21194350954&gbraid=0AAAADq98s_w1xD0mWL6E3f6_7x8BdP-1&gclid=Cj0KCQjw-pHPBhCdARIsAHXYWP8C7kIOOithlRw6xtxF9YcyZhO_iKefVFp-PiwJn3YbZ1eN8dBs8sgaApl_EALw_wcB

https://telkea.com/?gad_source=1&gad_campaignid=18946242871&gbraid=0AAAADRvSsUV1OUtZbSg3u8fEBxbHXtBY&gclid=Cj0KCQjw-pHPBhCdARIsAHXYWP84a-TC_cN48Hzb2hSl4YcxQKmF2TZlKicNNWAeaQRu9uUw9zq-wUQaAlDgEALw_wcB

6.La sécurité sur Internet

6.1. Le cryptage et les certificats HTTPS

https://www.primx.eu/fr/abc-chiffrement/chiffrement-composant-indispensable-de-la-protection-des-donnees/

https://www.mailinblack.com/ressources/glossaire/quest-ce-que-le-protocole-https/

https://www.hostinger.com/fr/tutoriels/site-non-securise-de-google-chrome

6.2. Les pares-feux et la protection des données

https://fr.wikipedia.org/wiki/Pare-feu_(informatique)

https://sirtel.tk/index.php/component/joomblog/show?show=3

https://www.fortinet.com/fr/resources/cyberglossary/how-does-a-firewall-work

6.3. Les menaces courantes (virus, piratage, phishing)

https://fr.wikipedia.org/wiki/Virus_informatique

https://www.kaspersky.fr/resource-center/definitions/what-is-hacking

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage

6.4. Risques et protection sur Internet

https://www.francenum.gouv.fr/guides-et-conseils/protection-contre-les-risques/cybersecurite/comment-se-proteger-sur-internet-et

https://www.kaspersky.fr/resource-center/definitions/the-ten-potentially-dangerous-things-you-do-onlinef

7.L’impact d’Internet sur la société

7.1. Communication, travail, et éducation

https://revue-histoire.fr/actualite-histoire/comment-internet-a-t-il-change-le-monde/?srsltid=AfmBOoq2xa6b5fso-amF4mcs0h4c6FdkniHm6TSyS4oHgUBbCy35wVhz

https://www.unesco.org/fr/digital-education

https://www.psychologue.net/articles/les-avantages-et-les-inconvenients-de-lutilisation-des-medias-sociaux-en-ligne

7.2. Les inégalités d’accès à Internet (fracture numérique)

https://fr.wikipedia.org/wiki/Fracture_num%C3%A9rique

https://www.actionenfance.org/les-dangers-d-internet-et-addiction-aux-reseaux-sociaux/

https://www.lelabocoworking.com/pourquoi-internet-est-devenu-un-element-essentiel-de-notre-quotidien/

7.3. L’avenir du réseau (Internet des objets, satellites, IA…)

https://fr.wikipedia.org/wiki/Internet_des_objets

https://innovsi.com/ia-intelligence-artificielle-joue-un-role-determinant-dans-la-transformation-digitale

https://www.omadanetworks.com/fr/blog/1702/quels-sont-les-d%C3%A9fis-%C3%A0-relever-en-terme-de-haute-densit%C3%A9-r%C3%A9seau-/

7.4. Les évolutions des réseaux de communication du futur

https://www.arcep.fr/uploads/tx_gspublication/reseau-du-futur-note-synthese_choisir-son-numerique_sept2025.pdf

https://www.cnrs.fr/fr/actualite/vers-des-reseaux-du-futur-flexibles-fiables-et-sobres

https://normandiewebschool.fr/blog/le-futur-des-reseaux-sociaux-a-quoi-sattendre-entre-2026-et-2030/