Modulo.

Une introduction à l'informatique

Groupe de travail DGEP, EPFL, HEP-VD, UNIL

17 juillet 2023

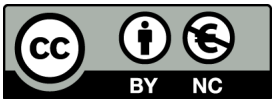


Table des matières

CHAPITRE **1**

Réseaux

Aujourd'hui quand nous parlons de **réseaux**, il n'est pas toujours clair s'il s'agit de réseaux sociaux, du web, de la 4G, du wifi ou plus généralement d'Internet, le réseau des réseaux. Dans ce chapitre, nous allons parler d'Internet, qui est une infrastructure permettant à des machines de communiquer entre elles sans être directement connectées entre elles.

1.0 Introduction

Internet est une infrastructure essentielle qui a complètement changé notre vie, que ce soit dans les relations sociales, l'éducation, la recherche, le commerce, la santé, etc. Dans ce chapitre, nous allons voir, dans les grands principes, comment Internet fonctionne et en quoi son fonctionnement est différent d'autres réseaux de communication qui l'ont précédé, tels que les réseaux postaux ou téléphoniques. En effet, une innovation majeure d'internet est qu'il s'agit d'un réseau *décentralisé*, et ceci explique dans une large mesure son succès et ce qu'il est devenu, même si certains craignent une recentralisation d'Internet autour des géants du numérique tels que Google et Amazon.

1.0.1 Origine d'Internet

Les réseaux de communication existaient bien avant Internet, par exemple :

- le réseau de télégraphie optique de Chappe (1794)
- le réseau de télégraphie électrique de Morse (1843)
- le réseau téléphonique de Bell (1877)
- le réseau de télégraphie par ondes radio de Marconi (1896)

Ces anciens réseaux avaient besoin d'opérateurs ou opératrices pour la transimssion des messages, ou, pour les plus récents, ils étaient centralisés. Cela signifie qu'il y a un point central du réseau par lequel passent toutes les communications. Après la 2e guerre mondiale, qui avait vu le nivellement de villes entières par des bombardements aériens (comme à Dresde) et la bombe atomique, l'armée américaine a décidé de financer

le développement d'un réseau de communication décentralisé (ou distribué), qui serait moins vulnérable à une attaque. L'idée était qu'un réseau de communication centralisé pouvait facilement être mis hors service par un adversaire en détruisant le point central, alors qu'un réseau de communication sans point central serait beaucoup plus difficile à attaquer.

Document historique

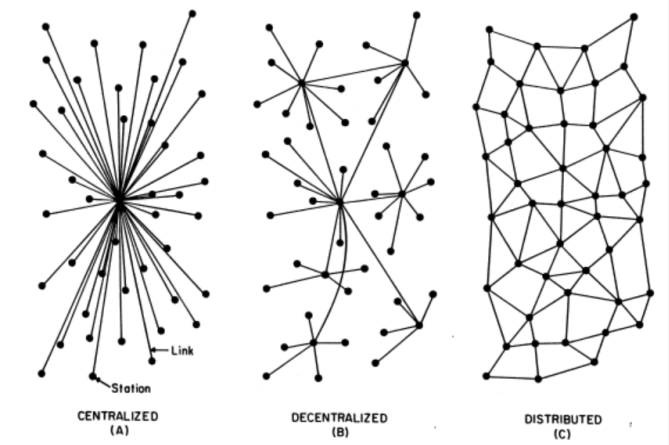


Fig. 1.1 – Image tirée de l'article proposant de réaliser un réseau décentralisé. Baran, *On Distributed Communications : I. Introduction to distributed communications networks*, RAND CORP CALIF, 1964, disponible ici[7]. Cette image illustre la différence entre un réseau centralisé (à gauche), dans lequel toutes les communications passent par un point central, et un réseau distribué (droite), dans lequel tous les noeuds ont plus ou moins la même importance. Le réseau du milieu représente un intermédiaire décentralisé, entre le réseau complètement centralisé de gauche et le réseau distribué de droite

Les universitaires américains ont été associés à la conception de ce réseau et l'ont utilisé pour partager des informations et des ressources entre universités. Ainsi est né Internet, par une association entre universitaires attachés surtout à la libre circulation de l'information et des militaires aux visées plutôt sécuritaires. Dès les années 70, le mouvement hippie, séduit par les possibilités d'auto-organisation et la philosophie non hiérarchique d'Internet a investi cette infrastructure et a développé une "cyberculture" qui marquera durablement l'histoire d'Internet, de l'émergence des réseaux sociaux aux cryptomonnaies. En 1983, les militaires ont déconnecté leur partie du réseau du reste d'Internet pour des raisons de sécurité.

1.0.2 Structure d'internet

Internet est souvent décrit comme un *réseau de réseaux*. En effet, Internet est construit sur une structure de *réseaux locaux* interconnectés les uns aux autres. Par exemple, les ordinateurs d'une école, d'une entreprise ou d'un appartement peuvent être reliés entre eux par le wifi, ou des câbles Ethernet et constituer un réseau local. Le réseau local est ensuite connecté, par le biais d'un *routeur*, au reste d'Internet. Ainsi Internet est constitué d'une myriade de sous-réseaux connectés (et potentiellement enchâssés) les uns aux autres. Ces réseaux sont connectés par les *dorsales d'Internet*, des câbles de fibre optique capables de transférer des données à haut débit, qui traversent les continents et les océans.

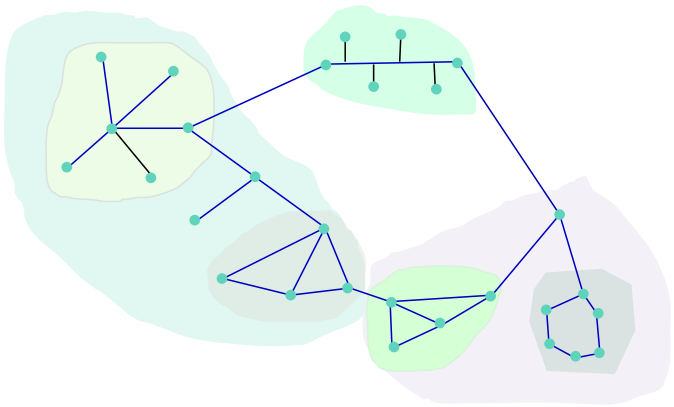


Fig. 1.2 – Un réseau de sous-réseaux. Les points représentent les machines, alors que les traits indiquent les connexions entre les machines. La couleur de fond indique les sous-réseaux.

Micro-activité – Les câbles sous-marins d'Internet

Aller sur le site https://www.fiberatlantic.com/submarinecablemap/ et regarder la carte des câbles sous-marins d'Internet. Trouver le câble qui relie l'Afrique du Sud à l'Inde. Comment s'appelle-t-il, depuis quand existe-t-il et quelle est sa longueur ? À qui appartient-il et quand est-il prévu de le mettre hors service ?

1.0.3 Fonctionnement d'Internet

Cette section présente une vue d'ensemble des éléments centraux du fonctionnement d'Internet et qui seront repris dans la suite du chapitre.

Adressage

Tout réseau de communication a besoin d'un système d'adresses afin de pouvoir distinguer et joindre les différents destinataires. Dans un réseau décentralisé qu'est Internet, le système d'adressage doit permettre à chaque machine connectée au réseau d'être identifiable et joignable, sans causer de quiproquo. Cela passe par une gestion hiérarchique des adresses.

Routage

Dans un réseau centralisé comme le téléphone traditionnel, un opérateur central (le standard dans le cas du téléphone) relie tous les appareils branchés au réseau. Lorsque deux personnes veulent entrer en communication, l'opérateur central les met en relation, c'est-à-dire relie leurs appareils. C'était d'abord fait à la main, puis automatiquement (avec le téléphone à cadran rotatif). Dans un réseau décentralisé, la mise en lien doit se faire de manière décentralisée. C'est ce qu'on appelle le *routage*.

Commutation par paquets

Dans un réseau centralisé comme le téléphone, lorsque deux personnes sont en communication, elles "occupent la ligne" : ces deux personnes ne sont pas joignables par d'autres personnes (c'est ce qu'indique le signal "occupé"), mais cela n'implique pas d'autres personnes qui veulent communiquer entre elles (sauf si le standard est surchargé). C'est ce qu'on appelle la *commutation de circuits*, car un circuit électrique est créé entre les deux appareils qui communiquent.

Imaginons maintenant qu'une relation soit établie entre deux appareils d'un réseau décentralisé. Si l'on avait une commutation de circuits, toutes les connexions utilisées pour acheminer l'information entre deux appareils seraient inutilisables pour les autres personnes utilisatrices du réseau, comme illustré dans la figure ci-dessous.

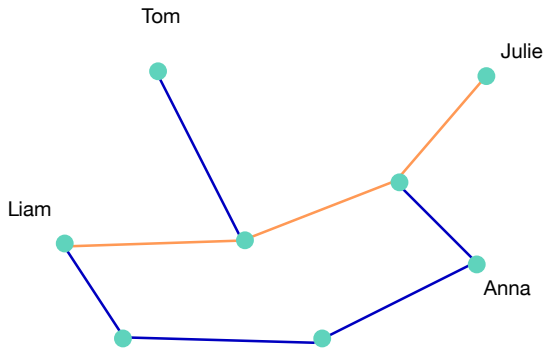


Fig. 1.3 – Si on réservait un circuit entre les ordinateurs de Liam et Julie (en orange) lorsque ceux-ci sont en communication par internet, Tom ne pourrait pas entrer en même temps en communication avec Anna, car tous les segments oranges seraient occupés.

Cela pourrait conduire rapidement à une saturation du réseau. Pour éviter ce problème, il a été décidé de "découper" la communication en petits morceaux (appelés les paquets) et d'envoyer chaque morceau individuellement. C'est ce qu'on appelle la *commutation par paquets*. C'est un peu comme si au téléphone on raccrochait et on se rappelait entre chaque mot. Cela ne monopolise pas la ligne et permet de mener plusieurs conversations en même temps sur la même ligne. En plus, cela ne sollicite la ligne que lorsqu'une information est transmise et pas, par exemple, pendant les moments de silence, ou lorsqu'on est en train de rédiger sa réponse sur une messagerie.

Les protocoles

Lorsque deux personnes entrent en communication, elles se mettent d'accord (souvent implicitement) sur la manière dont elles communiquent, par exemple la langue qu'elles vont utiliser, la manière dont on signifie le début et la fin d'une conversation (les salutations), etc. Pour les machines, ces règles doivent être précisées beaucoup plus en détails, car les machines n'ont pas la faculté d'interprétation et d'adaptation des humains. Dans un réseau décentralisé, il faut spécifier quels sont exactement les signaux que doit envoyer une machine qui veut se connecter au réseau et établir une communication avec une autre machine. C'est ce qu'on appelle le *protocole de communication*, par exemple comment la machine indique qu'elle veut établir ou fermer une communication, comment elle indique avec qui elle veut établir une communication, etc. Il y a pleins de protocoles différents, par exemple le protocole qui régit comment une machine veut se connecter par wifi à un routeur, le protocole qui régit comment demander le contenu d'une page web à un serveur (HTTP), le protocole qui régit comment envoyer un email sur le réseau (SMTP), ou se connecter à distance sur une

autre machine (SSH). Ces protocoles peuvent être ouverts (ou publics) est cela permet à chacun ou chacune de les utiliser, ou ils peuvent être fermés (ou privés) ce qui limite leur utilisation à l'entreprise ou l'entité qui les a inventés.

1.0.4 Organisation du chapitre

Dans le reste de ce chapitre, nous allons aborder plus concrètement les notions décrites ci-dessus et en approfondir certains aspects. Pour illustrer notre propos, considérons la situation suivante.

Ai-je compris ? – l'application aux champignons

Imaginons qu'Alice est partie à la cueillette aux champignons dans la forêt. Elle pense avoir trouvé un beau bolet, mais pour plus de sécurité, consulte avec son téléphone portable un site web spécialisé dans les champignons de notre région, *www.champignons.ch*. Que se passe-t-il réellement entre derrière l'écran de son téléphone ? C'est ce que nous allons découvrir dans ce chapitre.

1.1 Adressage

L'adresse est une notion importante en communication, qui permet à une personne ou une machine de s'adresser à une autre personne ou machine spécifique. Le rôle d'un système d'adressage, tel que celui de la poste, est de permettre d'identifier et de joindre une destination sans ambiguïté, et c'est pour ceci que chaque adresse doit être unique.

1.1.1 Les noms de domaine

Le nom *champignons.ch* est ce qu'on appelle un *nom de domaine*. Les noms de domaines sont gérés par l'ICANN, une organisation non gouvernementale à but non lucratif basée aux États-Unis dont la fonction principale est la gestion de l'adressage sur Internet. Les noms de domaines sont gérés de manière hiérarchique, selon le *nom de domaine de premier niveau*, c'est à dire la "terminaison" de l'adresse (*.ch*, *.org*, *.fr*, etc.) Ainsi la gestion des adresses en *.ch* est confiée à Switch, une fondation suisse dont c'est le rôle principal. La personne qui a créé le site *champignons.ch* a donc réservé ce nom de domaine auprès de Switch (en passant par un intermédiaire) et peut le conserver moyennant un paiement d'environ CHF 15.- par an.

Le saviez-vous ?

Au début, les noms de domaine de premier niveau étaient limités à quelques possibilités, telles que ".com" pour les organisations commerciales, ".edu" pour les universités (américaines), ".gov" pour le gouvernement (américain), ".mil" pour l'armée (américaine), ".org" pour les organisations (à but non lucratif) et, dès les années 80, différents pays ont décidé d'enregistrer des noms de domaine de premier niveau pour leur pays, par exemple ".ch" pour la Suisse, ".fr" pour la France. Puis il a été décidé d'ouvrir d'autres noms de domaine et de les mettre aux enchères. Une entreprise a alors décidé de vendre des domaines ".sucks" qu'elle a vendus très cher à certaines grandes entreprises (par exemple apple.sucks) qui avaient peur que ce site ne devienne une plateforme pour les critiquer.

Si les noms de domaines sont pratiques pour désigner des adresses sur Internet, les machines, elles, utilisent des nombres pour référencer les machines connectées à Internet, c'est ce qu'on appelle les *adresses IP*. Ainsi, la personne qui a enregistré le site *champignons.ch* a également reçu une (ou plusieurs) adresse IP de la part de Switch ou d'un intermédiaire.

Micro-activité

Déterminer à l'aide du site web https://www.nic.ch/whois/ qui a enregistré le nom de domaine champignons.ch.

1.1.2 Les adresses IP

Version 4 (IPv4)

Afin de pouvoir identifier chacune des machines connectées à Internet, il a été décidé de leur attribuer à chacune un nombre, un peu à la manière dont les numéros de téléphone sont attribués à chaque téléphone du réseau téléphonique. Dans sa version la plus courante, ce nombre est codé sur 32 bits, ce qui donne à peu près 4 milliards de possibilités (2^{32}). On pensait alors (c'était en 1982) que 4 milliards d'adresses seraient amplement suffisantes pour pouvoir accommoder toutes les machines pendant encore beaucoup d'années, et qu'Internet ne dépasserait pas les 4 milliards de machines connectées. A cette éqpoque, il n'y avait que quelques centaines d'ordinateurs connectés à Internet. Afin de rendre ces adresses plus lisibles pour les humains, on décompose d'habitude une adresse IP de 32 bits en quatre groupes de 8 bits séparés par un point. Chaque groupe de 8 bits peut alors être représenté comme un nombre décimal entre 0 et 255 ($2^8 - 1$).

Exercice 1

Lesquelles des adresses suivantes sont des adresses IP valides :

1. `240.264.23.2`
2. `123.8.12.2.34`
3. `123.23.2`
4. `205.233.12.23`

Version 6 (IPv6)

Avec le développement d'Internet, il est vite devenu clair que le nombre de machines connectées à Internet allait dépasser le nombre d'adresses IP différentes, et c'est pourquoi un nouveau type d'adressage a été développé dès les années 90, IPv6 (Internet Protocol, version 6). Il a été décidé de coder les adresses IP sur 128 bits. Plutôt que de les représenter avec 16 nombres entre 0 et 255, il a été décidé de coder en 8 nombres hexadécimaux entre 0000 et FFFF. Chaque chiffre de 0 à F représente ainsi 4 bits, et chaque nombre de 4 chiffres hexadécimaux représente donc $4 \cdot 4 = 16$ bits. En en prenant 8, on arrive bien à $8 \cdot 16 = 128$ bits.

Par exemple `4E3F.DEA7.409B.412C.2516.4A2B.2CFE.1282` pourrait constituer une adresse IPv6 valide. Elle est en effet constituée de 8 nombres à quatre chiffres hexadécimaux.

Actuellement, les deux types d'adresses IPv6 et IPv4 coexistent sur Internet, la version IPv4 étant encore largement plus répandue. Une adresse IP peut donc soit être sur 32 bits soit sur 128 bits.

Exercice 2

Parmi les adresses suivantes, indiquer lesquelles sont au format IPv4, lesquelles sont IPv6 et lesquelles ne sont pas valides. Justifier sa réponse.

1. `128.23.54.45`
2. `31.43.132.45.51.654.4355.4325`
3. `1923.2123.1323.4324.4241.2434.7657.5757`

4. `ADEFE.ACDEA.AABCD.DDEBC.FFEDA.AEABC.ACADE.EFDF`
5. `1230.121D.12AEAB.1231D.4324B.2765.5435D.4378`
6. `D2G3.4234.534FG.2141.12GE.12AD.85C2.GE32`
7. `123A.3213.564E.6746.2DD2.A897`
8. `124.234.432.21`

Gouvernance

Comme les noms de domaine, les adresses IP sont gérées hiérarchiquement. Ainsi, les adresses IPv4 de la forme `46.x.x.x` (c'est-à-dire celles qui commencent par `46 = 00101110`) sont assignées au Centre de Coordination Européen qui les répartit entre différents *Registres Internet locaux* tels que Switch qui va pouvoir louer une partie de ces adresses IP à des organisations, des entreprises (par exemple des fournisseurs d'accès Internet) ou des particuliers qui en feraient la demande.

Certains blocs d'adresses IP sont réservés à des usages particuliers. Par exemple les adresses `10.x.x.x` ou `192.168.x.x` sont réservées aux réseaux privés, c'est-à-dire des machines qui ne communiquent pas directement avec le reste d'Internet. Ainsi, ces adresses peuvent être utilisées au sein du réseau interne des entreprises, ou pour faire communiquer différents appareils connectés (imprimante, télévision, ordinateurs, ou smartphones) au sein d'une maison. Dans l'exemple ci-dessous, un fournisseur d'accès à Internet (tel que Swisscom par exemple) à reçu toutes les adresses de type 213.221.x.x. Il en garde une partie pour son propre usage, par exemple pour son site web et les machines qui opèrent le réseau. Une autre partie des adresses sera louée à des entreprises ou des particuliers qui sont ses clients. Ceux-ci bénéficieront donc d'une adresse IP leur permettant d'être joignables par le reste d'Internet.

Micro-activité

— Déterminer à l'aide de cette page Wikipedia [2] à quel continent sont allouées les adresses IP suivantes :
  — 212.x.x.x
  — 154.x.x.x
  — 20.x.x.x
— Déterminer à l'aide de ce site [3] l'entité suisse qui possède le plus d'adresses IP

2. https://en.wikipedia.org/wiki/List_of_assigned_/8_IPv4_address_blocks
3. https://www.nirsoft.net/countryip/ch.html

Exercice 3

— Combien y a-t-il d'adresses IP de type `192.168.x.x` ?
— Combien y aurait-il eu d'adresses IP possibles s'il avait été décidé de l'encoder sur 24 bits ?
— Donnez la représentation binaire de l'adresse IP `10.0.45.12`

Réseau privé

Les particuliers et entreprises ont généralement un réseau privé, un *intranet*, qui utilise les adresses 10.x.x.x. L'appareil qui permet de connecter ce réseau privé au reste d'Internet est un *routeur*, par exemple la boîte wifi qui est fournie par le fournisseur d'accès. Ce routeur a à la fois une adresse locale (dans notre exemple 10.0.1.1) pour être joignable depuis le réseau privé et une adresse globale (213.221.190.41 dans l'exemple ci-dessous) pour être atteignable depuis le reste d'Internet. Le routeur joue un peu le rôle du secrétariat de l'école en s'occupant de transmettre le courrier entre l'intérieur et l'extérieur de l'école. De manière similaire, le secrétariat a d'habitude deux boites aux lettres, une pour les documents déposés par des personnes qui sont à l'intérieur de l'école (élèves, personnel enseignant) et une destinée au facteur qui amène le courrier en provenance de l'extérieur du gymnase.

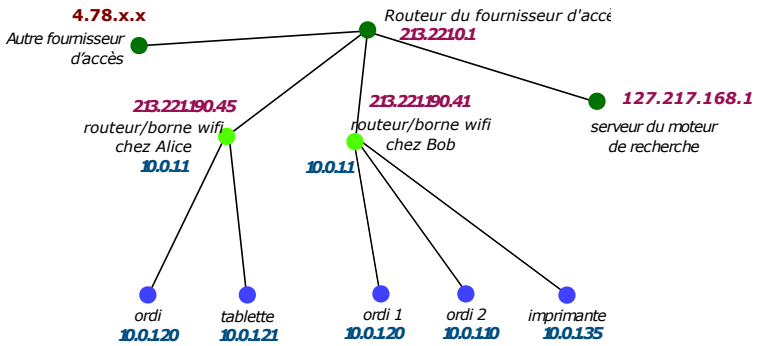


Fig. 1.4 – Exemple de distribution des adresses IP, avec un fournisseur d'accès ayant obtenu les adresses 213.221.x.x, rt qui fournit un accès Internet à Alice et Bob. Les routeurs, en vert clair, ont deux adresses IP.

Micro-activité

- A l'aide d'un navigateur web, aller sur le site https://www.whatismyip.com et déterminer sa propre adresse IP.
- Dans un terminal taper la commande suivante qui détermine votre adresse IP :
  - sur Mac Os ou Linux : `ipconfig getifaddr en0`
  - sur Windows : `ipconfig`
- Obtient-on la même réponse ? Pourquoi ?

Adressage statique et dynamique

Une adresse IP peut être allouée de manière *statique* ou *dynamique*. Dans le cas de l'adressage statique, on configure la machine en lui indiquant son adresse IP, est c'est elle qui annonce au réseau quelle est son adresse IP, afin que les messages puissent lui parvenir. La machine conserve ainsi toujours la même adresse IP, de la même façon qu'un téléphone conserve toujours le même numéro (sauf si on le reconfigure en modifiant par exemple la carte SIM). Dans le cas de l'adressage dynamique, la machine demande une adresse IP au moment où elle se connecte à Internet. Cette demande se fait auprès d'un serveur qui va lui allouer une adresse IP disponible parmi celles qu'il a à disposition. C'est un peu comme si chaque fois qu'on allumait son téléphone, on recevait un autre numéro pour être joignable. Si c'est nous qui initions les appels, cela ne pose pas vraiment de problème, mais si on veut être joignable, cela devient problématique, car les autres ne sauront pas comment nous trouver. Mais cela a d'une part l'avantage d'éviter qu'une machine non connectée monopolise une adresse IP sans l'utiliser et d'autre part, cela donne un (petit) degré d'anonymat et de sécurité en plus, car il sera plus difficile de cibler précisément notre machine et intercepter nos messages sur Internet.

Ainsi les serveurs (les sites web, par exemple), qui doivent être joignables en tout temps ont généralement une adresse IP statique, alors que les machines des utilisateurs et utilisatrices ont souvent une adresse IP dynamique. Lorsqu'on fait un abonnement Internet, le fournisseur d'accès propose d'habitude une adresse IP dynamique (cela lui permet d'économiser les adresses IP en sa possession), mais il est également possible, en payant un peu plus, d'obtenir une adresse IP statique.

Micro-activité

En regardant les paramètre réseaux, déterminer si sa machine a une adresse IP statique (manuel) ou dynamique (DHCP).

Exercice 4

1. Vous souhaitez entrer en communication avec votre ami-e, mais vous avez les deux des adresses IP dynamiques. Quel moyen pourriez-vous imaginer pour que vous puissiez vous joindre.
2. En tant que propriétaire d'un site web, vous avez accès aux adresses IP des machines qui visitent votre site. Pouvez-vous dès lors identifier une même personne qui revient plusieurs fois sur votre site ?
3. Depuis votre adresse IP dynamique, vous être entré en communication avec un site web illégal. La police peut-elle vous retrouver à partir de votre adresse IP ? Si oui comment, si non pourquoi ?

Solution 4

1. Vous pouvez vous connecter tous deux à un serveur central qui a une adresse IP fixe et qui s'occupera de relayer vos messages à vos adresses dynamiques. C'est ce que fait un serveur mail ou de messagerie telle que Signal ou Whatsapp.
2. Si elle a une adresse IP dynamique, alors elle aura probablement des adresses IP différentes lors de ses visites en des jours différents. On ne pourra donc pas l'identifier en regardant uniquement son adresse IP. Par contre, en enregistrant d'autres paramètres que son navigateur voudra bien nous transmettre, tels que son système d'exploitation, la langue, l'appareil, etc., on peut reconstituer son empreinte numérique et l'identifier ainsi. C'est ce qu'on appelle en anglais le fingerprinting, que l'on peut bloquer avec certains navigateurs [4].
3. Oui, votre fournisseur d'accès à Internet doit garder une trace de quelle adresse IP a été allouée à qui et à quel moment. La police peut dès lors exiger ces informations en cas de soupçons.

4. https://www.mozilla.org/fr/firefox/features/block-fingerprinting/

1.1.3 Système de noms de domaine

Pour récapituler ce qui a été vu précédemment, les humains utilisent les noms de domaines pour les machines, alors que les machines, elles, utilisent les adresses IP. Afin que ces deux modes de recensement des machines soient cohérents entre eux, il est nécessaire de disposer d'un annuaire qui fera correspondre les noms de domaines aux adresses IP. Ceci est analogue aux annuaires téléphoniques ou aux contacts du smartphone qui permettent de faire correspondre le nom des personnes que l'on veut atteindre (qui serait équivalentes au nom de domaine) au numéro de téléphone (qui est analogue à l'adresse IP). Cet annuaire est ce qu'on appelle le *système de noms de domaine* (Domain Name System ou DNS selon l'appellation anglaise). Au début d'Internet, il s'agissait simplement d'un fichier texte librement accessible qui listait le nom de domaines et les adresses IP correspondantes. Ce fichier était maintenu à la main. Maintenant, il s'agit de machines, les serveurs DNS dans le réseau auprès desquelles il est possible d'obtenir l'adresse IP correspondante à un nom de domaine.

Ces machines sont aussi organisées hiérarchiquement de telle sorte que chaque serveur DNS ne stocke que les noms de domaines correspondant à une sous-partie du réseau.

Le saviez-vous ? – Le hacking de DNS

Une méthode de hacking consiste à mettre en ligne un serveur DNS malveillant qui va diriger le traffic vers des faux sites web se faisant passer pour des vrais. Par exemple, un hacker pourrait mettre en ligne un DNS malveillant indiquant une fausse adresse IP pour le site google.com, et à cette adresse, mettre un serveur web ayant la même page d'accueil que Google. Lorsque une quelqu'un essaiera de se connecter à son compte google sur le faux site, ce site enregistrera simplement le login et mot de passe et renverra sur le vrai site web. Le hacker aura ainsi le login et mot de passe du compte google de la personne, pouvant ainsi avoir accès à ses emails et documents. La difficulté pour le hacker est de "convaincre" que son serveur DNS est fiable.

Le saviez-vous ? – La censure par le DNS

Une des méthodes à disposition d'un état qui souhaite empêcher ses habitants d'accéder à certains sites consiste à interdire aux serveurs de DNS du pays de répondre correctement aux requêtes concernant certains noms de domaine, voire de renovoyer des fausses adresses IP lorsque les requêtes DNS sont interceptées. En Chine, par exemple, Facebook.com est interdit, et les DNS chinois vont refuser de retourner l'adresse IP du site de Facebook. Cette censure peut parfois être contournées en recourant à des serveurs DNS situés à l'extéreur du pays.

Ai-je compris ? – L'exemple d'Alice

L'organisation qui a développé l'application aux champignons, a obtenu le nom de domaine *champignons.ch* et une adresse IP statique. Pour qu'Alice puisse aller sur ce site, son téléphone va envoyer une requête à un serveur DNS avec le nom de domaine "champignons.ch". Cette requête transitera par différents serveurs DNS organisés hiérarchiquement jusqu'à ce qu'un serveur DNS puisse y répondre, et la réponse sera retransmise jusqu'au téléphone d'Alice. Le téléphone d'Alice a lui aussi reçu une adresse IP dynamique de la part de son opérateur téléphonique afin que le serveur web puisse lui envoyer la page web du site.

1.2 Paquets et protocoles

Une fois que l'on connait l'adresse d'un destinataire, il est possible d'établir un contact et de lui transmettre de l'information. Sur Internet, ceci se fait en découpant cette information en petits paquets que l'on étiquette de façon bien précise. La manière dont ceci se fait est définie par les *protocoles* d'Internet.

1.2.1 Les paquets

Dès leur origine, les systèmes de communication se sont développés selon deux modes distincts selon les supports utilisés. Soit on maintient un "canal de communication" ouvert par exemple avec le téléphone ou la communication radio (le talkie-walkie). Dans ce cas, le récepteur et l'émetteur entrent en communication et l'information est envoyée de manière continue de l'émetteur au récepteur. Le récepteur ne peut pas être en communication avec plusieurs émetteurs à la fois. Dans le second cas de figure, par exemple le courrier postal ou le télégramme, les informations sont envoyées "en bloc", typiquement par messages acheminés en une fois. Dans ce cas, le récepteur peut recevoir des messages de différentes personnes de manière presque simultanée, et le fait d'envoyer un message à quelqu'un ne va pas empêcher quelqu'un d'autre d'entrer en communication et nous envoyer des messages.

Afin d'éviter de bloquer les lignes de communication, Internet s'est développé selon ce second mode, et c'est pourquoi il était justifié d'évoquer ci-dessus des *messages* qui étaient envoyés et circulaient dans le réseau. En effet, toute information envoyée par Internet est découpée en petits *paquets* qui sont envoyés indépendamment les uns des autres. Ainsi, lorsque le serveur hébergeant le site www.champignons.ch va envoyer une image de champignon à Alice, cette image sera découpée en petits paquets qui seront chacun envoyés séparément à Alice. Cela a l'avantage que si, pour une raison ou une autre, une partie de l'image se perd en route, il n'y a pas besoin de renvoyer toute l'image, mais uniquement les parties qui se sont perdues. Cela permet aussi à une machine de maintenir plusieurs canaux de communications ouverts simultanément. C'est ce qu'on appelle la *commutation par paquets* parce que ce sont les paquets qui sont adressés individuellement à leur destinataire. À l'inverse, dans le cas du téléphone traditionnel, lorsqu'on appelle quelqu'un, un circuit électrique est établi entre les deux téléphones pour leur permettre de communiquer (à l'exclusion des autres téléphones), c'est ce qu'on appelle la *commutation de circuits*.

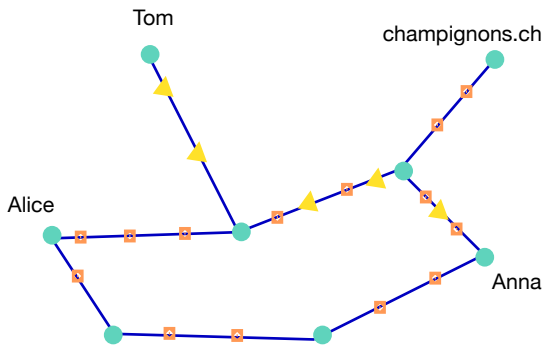


Fig. 1.5 – Les données envoyées de Alice à *champignons.ch* sont découpées en petits paquets (représentés par des carrés orange). Cela permet de partager les lignes avec d'autres utilisateurs et utilisatrices tels que Anna et Tom qui communiquent également en s'envoyant des paquets (représentés par des triangles jaunes). On peut noter que ces paquets ne prennent pas tous forcément le même chemin pour arriver à destination.

Les protocoles IP (Internet Protocol) et TCP (Transmission Control Protocol) décrivent le format ainsi que la gestion possible de ces paquets.

1.2.2 Le protocole IP

L'envoi d'un paquet par la poste suit certaines règles, telles que la position et le format de l'adresse de destination, la position et le format de l'adresse d'expédition, la position du timbre et son montant en fonction du poids et de la destination. Sans ces règles, l'acheminement du paquet ne peut pas être assuré. De manière analogue l'envoi d'un paquet sur Internet doit suivre certaines règles pour être acheminé. C'est le protocole IP qui définit ces règles.

Selon ce protocole un paquet est constitué d'une suite de 0 et de 1 que l'on peut séparer en deux parties.

1. L'entête qui donne des informations sur le paquet (son émetteur, sa destination, sa taille, etc.)
2. Les données (appelées aussi la *charge utile*) qui forment le contenu du paquet, c'est-à-dire les informations que l'on veut transmettre.

L'entête joue le rôle de l'étiquette sur un paquet envoyé par la poste. On y indique l'adresse de destination, l'adresse de l'expéditeur (appelée aussi l'adresse source), mais aussi d'autres informations telles que la version d'IP utilisée (4 ou 6), la longueur totale du paquet, ainsi que sa "durée de vie". Sa durée de vie indique au bout de combien de temps le paquet peut être abandonné pour éviter d'avoir des paquets qui circulent indéfiniment sans trouver leur destinataire. Dans la version IPv4, l'entête fait au minimum 20 octets, remplis comme dans l'image ci-dessous.

En-tête IPv4

0 1 2 3	4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version d'IP	Longueur de l'en-tête	Type de service	Longueur totale en octets
Identification			Indicateur / Fragment offset
Durée de vie		Protocole	Somme de contrôle de l'en-tête
Adresse source			
Adresse destination			
Option(s) + remplissage			

Ainsi, les 4 premiers bits indiquent la version d'IP utilisée (donc 0100 si c'est la version 4), les quatre suivants donnent la longueur de l'entête en lignes de 32 bits, et la longueur totale (en octets) du paquet est données par les troisième et quatrième octets de l'entête IP. L'adresse IP de la source occupe les octets 13 à 16, et celle de la destination les octets 17 à 20.

Exercice 1

Un paquet avec l'entête IP suivante (en hexadécimal) circule sur Internet :

```
45 00 00 14 00 01 00 00 0A 00 BF 88 C1 C8 DC EA 91 E8 C0 C5
```

Déterminer de quelle version de protocole IP il s'agit, la longueur du paquet ainsi que les adresses IP (en binaire) de l'émetteur et du recepteur.

Solution 1

Chaque chiffre hexadécimal représente 4 bits, et donc chaque nombre à deux chiffre représente un octet (8 bits). Selon la spécification de l'entête, d'IP est donnée par les 4 premiers bits, donc le premier chiffre de l'entête qui est 4. C'est donc en entête en IPv4. La longueur du paquet est donnée en hexadéximal par les octets 3 et 4, donc `00 14` c'est à dire 20 octets (en décimal). Ce paquet ne contient donc pas de données. L'adresse de l'émetteur (l'adresse source) est donnée à la quatrième ligne de 32 bits (ou 4 octets), c'esr donc `C1 C8 DC EA` en hexadécimal, c'est à dire `1100 0001 1100 1000 1101 1100 1110 1010` en binaire. La ligne suivante donne l'adresse de destination qui est `91 E8 C0 C5` en hexadécimal ou `1001 0001 1110 1100 0000 1100 0101` en binaire.

1.2.3 Le protocole TCP

Contrairement à une lettre dans laquelle on peut écrire tant qu'on veut, un paquet IP a une taille maximale fixe de 65535 octets, et donc on sera parfois obligé de découper une information (par exemple une image ou une vidéo) en plusieurs paquets IP afin de l'envoyer. Le récepteur doit ensuite reconstruire l'information à partir des paquets reçus et confirmer qu'il a bien tout reçu et que rien n'a été perdu en route (ce qui arrive parfois, comme avec la poste). Le protocole TCP (Transmission Control Protocol) permet aux machines réceptrice et émettrice de s'assurer que l'information a bien été transmise et reconstituée.

Pour ceci, l'information est découpée en morceaux de taille inférieure à la taille maximale des paquets IP, et chaque morceau est numéroté (avec des nombres consécutifs) et envoyé dans un paquet IP. La machine réceptrice sait ainsi comment reconstituer l'information et peut vérifier qu'il ne lui manque pas de morceaux.

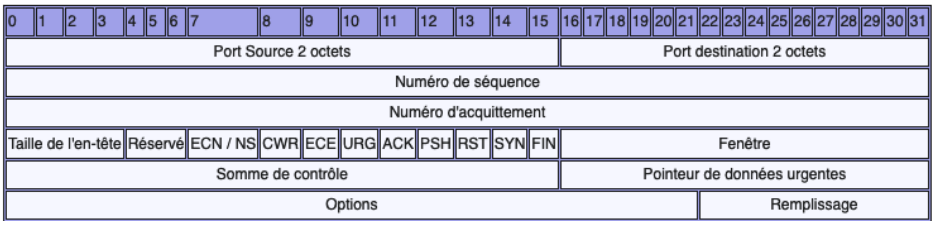
Exercice 2

On désire envoyer par email une photo de 2 Mo. De combien de paquets au minimum aura-t-on besoin pour envoyer cette photo ?

Entête

De manière similaire au protocole IP, le protocole TCP est constitué d'un *entête* placé au début des données du paquet IP et qui contient des informations sur les numéros de morceaux envoyés et reçus. En effet, la machine réceptrice va envoyer une quittance (*acknowledgement* en anglais) pour chaque paquet reçu, de manière à ce que la machine émettrice puisse renvoyer un paquet qui n'aurait pas été acheminé à destination. Un paquet envoyé par les protocoles TCP et IP, contient donc l'entête IP, suivi de l'entête TCP, suivi des données, tel que représenté ci-dessous.

L'entête TCP est constitué d'au moins 20 octets contenant les informations suivantes :



Comme le montre la figure ci-dessus, les quatre premiers octets contiennent les ports source et de destination. Un port est un peu comme une boîte aux lettres à l'intérieur d'un ordinateur. Les ports sont numérotés sur 16 bits, donc de 0 à $2^{16} - 1$. Un ordinateur qui est en connexion simultanée avec plusieurs ordinateurs pourra par exemple assigner un port différent à chaque connexion, ce qui lui permettra de ne pas mélanger les messages reçus de ses divers interlocuteurs. Dans ce contexte et contrairement à un port USB, un port n'a pas de réalité matérielle, il est réalisé de manière logicielle par le système d'exploitation.

Les quatre octets suivants contiennent le numéro de séquence qui va permettre au programme qui reçoit les paquets de les remettre dans l'ordre selon ce numéro. Le numéro d'acquittement sont utilisés par le destinataire pour indiquer quels sont les paquets qui ont été reçus, permettant ainsi à la machine émettrice de savoir quels paquets se sont perdus en chemin et doivent être envoyés à nouveau. Les quatre octets suivants contiennent divers éléments permettant aux deux machines en communication de se synchroniser, notamment divers fanions indiquant si on veut initier, ou terminer la connexion, ainsi que "Fenêtre" par lesquels le récepteur indique à l'émetteur combien de place il lui reste dans la pile des paquets à trier et traiter. Ceci permet à l'émetteur d'adapter le rythme auquel il envoie les paquets pour ne pas déborder le récepteur. Enfin la "Somme de contrôle" est un code correcteur d'erreur qui permet de vérifier si l'entête n'a pas été altéré en chemin.

Exercice 3

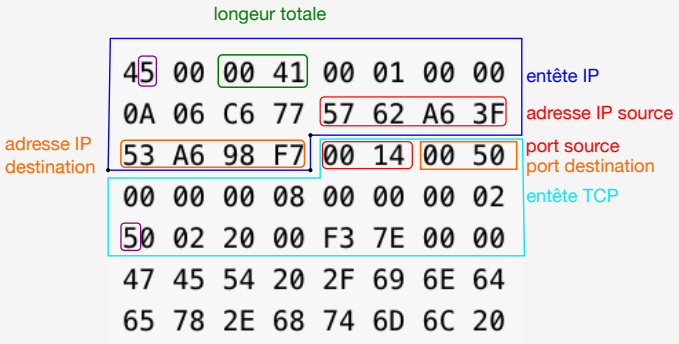
Un paquet a été intercepté sur Internet avec le contenu initial suivant indiqué en hexadécimal :

```
45 00 00 41 00 01 00 00
0A 06 C6 77 57 62 A6 3F
53 A6 98 F7 00 14 00 50
00 00 00 08 00 00 00 02
50 02 20 00 F3 7E 00 00
47 45 54 20 2F 69 6E 64
65 78 2E 68 74 6D 6C 20
```

1. Déterminer quelle partie de cet entête correspond à l'entête IP, et laquelle correspond à l'entête TCP.
2. Indiquer l'adresse IP et le port de l'émetteur de ce paquet.
3. Indiquer l'adresse IP et le port du destinataire de ce paquet.
4. Quelle est la longueur du paquet ?
5. Combien d'octets du paquet ne sont pas représentés ci-dessus ?

Solution 3

1. Le premier chiffre de l'entête étant un 4, c'est le format IPv4. La taille de l'entête IP est donc donnée par les bits 4 à 7, et donc le deuxième chiffre hexadécimal de l'entête qui est un 5 (en mauve). L'entête IP correspond donc aux 5 premiers mots de 32 bits, c'est-à-dire aux 20 premiers, octets donc aux 20 premiers nombres à 2 chiffre hexadécimaux (en bleu dans l'image ci-dessous). L'entête TCP suite directement et sa taille est donnée par le début du 13e octet, qui est un `5` (en mauve) dans notre exemple. L'entête TCP fait donc également $5 \cdot 4 = 20$ octets, en cyan. L'image ci-dessous indique comment interpréter cet entête.

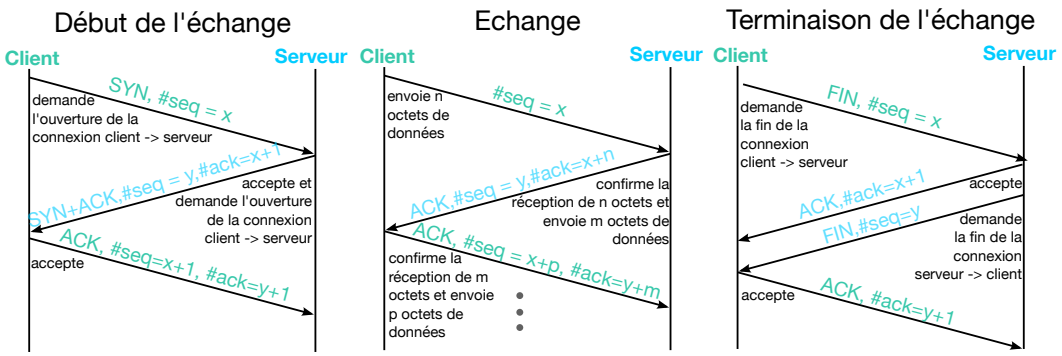


1. L'adresse IP de la source en hexadécimal est `57 62 A6 3F` ou `87.78.166.63` en notation usuelle. Le no de port est `0014` en hexadécimal, donc $1 \cdot 16 + 4 = 20$ en décimal.
2. L'adresse IP du destinataire en hexadécimal est `53 A6 98 F7` ou `83.166.152.247` en notation usuelle. Le no de port est `0050` en hexadécimal, donc $5 \cdot 16 + 0 = 80$ en décimal.
3. La longueur totale est de $41_{16} = 4 \cdot 16 + 1 = 65$ octets, y compris l'entête.
4. Seuls 56 octets sont représentés ci-dessus, il manque donc $65 - 56 = 9$ octets.

Déroulement

Le protocole TCP applique une structure *client-serveur* à communication entre deux machines. Cela signifie qu'une des machines, appelées le serveur, va se mettre en mode d'écoute, et attendre que d'autres machines la contactent. C'est la machine cliente qui va prendre l'initiative d'initier la communication en envoyant un message TCP (juste l'entête, sans les données) à la machine serveur. Le protocole TCP spécifie les messages qui doivent être envoyés de part et d'autre pour initier la connexion, comment ensuite envoyer et quittancer les données échangées, et comment mettre fin et terminer la connexion une fois que tout a été envoyé et quittancé.

La figure ci-dessous indique comment les fanions SYN, FIN de l'entête TCP sont utilisés pour indiquer que l'on veut respectivement initier et terminer une connexion, et comment le fanion ACK est utilisé pour confirmer la bonne réception de la demande ou des données, avec les numéros des séquences (#seq) et et d'acquittement (#ack).



Exercice 4

Un serveur reçoit un paquet TCP avec le contenu suivant dans l'entête. Que cela signifie-t-il, et comment le serveur est-il censé réagir si tout se passe bien ?

1. FIN = 1, no de séquence = 257
2. SYN = 1, no de séquence = 745
3. ACK = 1, no de séquence = 343, no d'acquittement = 746,

Solution 4

1. Le client souhaite mettre fin à la connexion. Le serveur répond avec ACK=1, no d'acquittement=258
2. Le client souhaite établir une connection, le serveur répond avec SYN=1, ACK=1, no d'acquittement=746 et un no de séqence.
3. Le client a reçu les paquets jusqu'à l'octet 746 (non compris) et envoie un message numéroté 343. Le serveur envoie un paquet avec l'ACK=1, no d'acquittement 343+m. S'il y a p octet à envoyer le serveur l'inclut et un no de séquence 746+p.

Exercice 5

— Quelle est no de séquence maximal que l'entête TCP peut contenir ?
— Que peut-on faire si le nombre de paquets envoyés est tel que ce nombre est dépassé ?

1.2.4 Le protocole UDP

TCP n'est pas l'unique moyen de transmettre des messages par internet. Par exemple, si l'important est que les données soient transmises rapidement, même si certaines sont perdues en route, on peut utiliser le protocole UDP. Avec ce protocole, l'émetteur envoie des paquets au destinataire sans vérifier que ce dernier les reçoit, ou même qu'il est présent à l'adresse de destination. L'entête UDP ne contient que quatre champs de 2 octets chacun, déjà présent dans l'entête TCP.

2 octets	2 octets	2 octets	2 octets
port source	port destination	longueur totale	somme de contrôle

Il n'y a donc pas de numérotations des séquences, ni de système d'acquittement, ce qui fait que si un paquet est perdu ou s'arrive en retard par rapport aux autres paquets, on l'expéditeur et le destinataire n'ont aucun moyen de le savoir. Par contre, cela permet d'aller plus vite, donc ce protocole est surtout utilisé dans les applications en temps réel.

Exercice 6

Indiquer pour les applications suivantes, si le protocole TCP ou UDP était plus adapté, et indiquer pourquoi.

1. La lecture d'une page web
2. Une application de téléphonie par Internet
3. Le streaming d'une vidéo
4. Une application bancaire en ligne
5. Un jeu vidéo en ligne

Ai-je compris ? – L'exemple d'Alice

Pour entrer en communication avec le serveur web, le téléphone d'Alice va utiliser le protocole TCP. Le téléphone va donc créer un entête TCP dans lequel il indiquera (par l'utilisation du fanion SYN) qu'il souhaite établir une connection avec le site web. Devant cet entête il mettra également un entête IP dans lequel il indiquera (entre autres) les adresses IP du téléphone d'Alice (comme source) et du site web (comme destination). Ces deux entêtes formeront un paquet IP qui sera envoyé à travers le réseau jusqu'au serveur web qui répondra par un autre paquet, selon le protocole TCP. Une fois la connection établie, le navigateur web d'Alice pourra demander au serveur le contenu de la page web. Celle-ci sera découpée en petit morceaux qui seront numérotés et envoyés séparément au téléphone d'Alice qui enverra des acquittement pour les paquets reçus. Le serveur pourra ainsi renvoyer les paquets pour lesquel il n'a pas reçu d'acquittement.

1.3 Routage

Le **routage** est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à une destination.

Pour comprendre le routage, il faut distinguer deux types de machines qui font fonctionner Internet :

— le **routeur**, qui sert d'intermédiaire dans la transmission d'un message,

— l' **hôte** qui émettent ou reçoivent un message.

1.3.1 Les routeurs

Les *routeurs* sont des ordinateurs spécialisés dont le rôle est de relayer et d'orienter correctement les informations qui circulent sur Internet. Si Internet est représenté par un graphe dont les arêtes représentent les canaux de communication, alors les routeurs sont situés aux noeuds du graphe et décident dans quelle direction faire suivre une information afin qu'elle atteigne son destinataire. Les routeurs sont donc comme des facteurs disposés aux intersections du réseau Internet qui vont lire la destination des messages qui leur arrivent et les rediriger vers la prochaine intersection de manière à les rapprocher de leur destination. Les hôtes sont généralement aux l'extrémités du graphe.

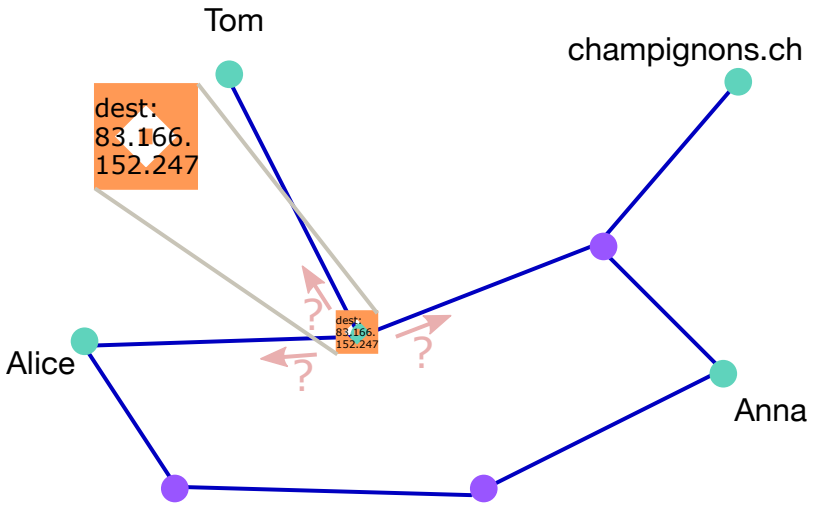


Fig. 1.6 – Un routeur regarde le destinataire de chaque paquet qu'il reçoit et le redirige dans la bonne direction vers le prochain routeur ou le destinataire. Dans notre exemple, le paquet de données (représenté par le carré orange) qu'Alice veut envoyer au serveur champignons.ch transite par différents routeurs (représenté en violet), qui décident par où faire transiter le message en fonction de l'adresse de destination du paquet.

Pour ceci, les routeurs s'aident de *tables de routage* qui leur indique la direction à suivre pour chaque destination.

1.3.2 Les tables de routage

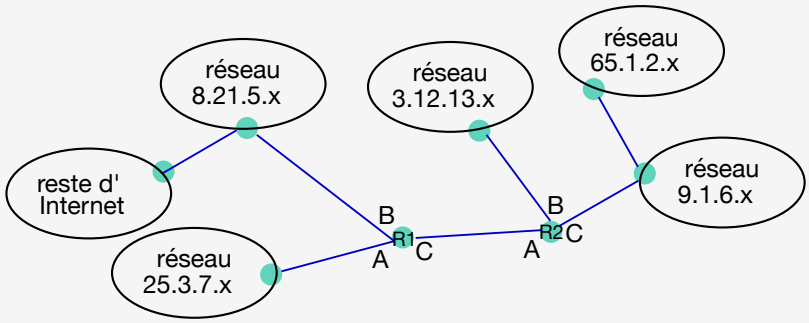
Une table de routage est un tableau qui indique dans quelle direction orienter un message en fonction de son destinataire. Conceptuellement, on peut imaginer une table de routage comme un tableau à deux colonnes, la première colonne contenant l'adresse IP de destination (ou un sous réseau à laquelle elle appartient), la seconde colonne indiquent *l'interface* à laquelle il faut envoyer les messages destinés à cette adresse. L'interface représente la "direction" dans laquelle envoyer le message (par exemple un port Ethernet, un câble en fibre optique, un émetteur wifi). Ainsi lorsqu'un nouveau message atteindra le routeur, celui-ci regardera dans sa table de routage la ligne contenant le sous-réseau le plus spécifique incluant l'adresse IP de destination et le fera suivre dans l'interface correspondante (qui est elle-même connectée soit à un autre routeur soit au destinataire).

Destinataire	Interface
127.1.1.1	A
34.234.15.x	B
87.45.x.x	C
87.33.x.x	C
x.x.x.x	D

La dernière ligne représente la *passerelle par défaut* qui indique où envoyer les messages dont l'adresse ne correspond à aucune autre ligne de la table.

Exercice 1

Remplir les tables de routage simplifiées des routeurs R1 et R2 du réseau suivant dans lequel les interfaces sont représentées par les lettres A,B, et C.



Les tables de routage contiennent souvent des informations, c'est-à-dire des colonnes, supplémentaires. Elle peuvent par exemple contenir une colonne "Distance" qui indique le nombre de d'étapes avant d'arriver à destination. Les voisins directs sont ainsi une distance de 1, alors que les voisins des voisins ont une distance de 2, etc. D'autres informations peuvent figurer comme le coût de transmission d'un paquet, ou le traffic maximal que cette route peut supporter.

Exercice 2

Ajouter une colonne "Distance" à la table de routage de l'exercice précédent.

Pour aller plus loin – Masques de réseau

Pour qu'une machine sache si une autre machine est dans le même sous-réseau qu'elle, son sous-réseau est spécifié par un *masque* de réseau composé d'une suite de 32 bits (en IPv4) dont les n premiers sont à 1 et les $32-n$ suivants sont à 0. Par exemple, une machine peut avoir une adresse IP 128.178.23.132 avec un masque de 11111111.11111111.1111111.000000000. Cela signifie que toutes les machines qui ont la même adresse IP là où le masque vaut 1 sont dans le même sous-réseau. Dans notre exemple, cela correspond à toutes les adresses IP 128.178.23.x. Pour gagner de la place, les masques sont aussi exprimés en 4 nombres décimaux, dans notre exemple 255.255.255.0, ou alors, pour faire encore plus court, on peut simplement spécifier le nombre de 1 du masque, ce qui donne, toujours pour le même exemple, 128.178.23.132/24.

Ainsi toutes les adresses IP qui n'a pas les mêmes n premiers bits, fait partie d'un différent sous-réseau. Pour lui envoyer des paquets, il faudra passer par la *passerelle par défaut* (*default gateway* en anglais) qui est le routeur qui s'occupe de communiquer avec l'extérieur du sous-réseau.

Dans des petits réseaux locaux, cette table de routage peut être construite manuellement, mais généralement c'est le routeur qui construit sa propre table de routage en interaction avec les routeurs voisins.

1.3.3 Le routage dynamique

Dans la pratique, le réseau de connections qui constituent Internet change et évolue constamment : de nouvelles machines se connectent au réseau, changent d'adresse IP, des routeurs tombent en panne, certaines connexions s'ajoutent ou disparaissent, par exemple en cas de dommages aux câbles. Cela ne serait pas gérable pour des humains de constamment mettre à jour les tables de routage pour les adapter à la configuration du réseau. C'est pourquoi un système automatisé de mise à jour des tables de routage est utilisé. C'est ce qu'on appelle le *routage dynamique*. Cela permet non seulement de gérer les changements configuration du réseau, mais également les phénomènes de congestion du trafic.

Le protocole RIP

Le protocole RIP (Routing Information Protocol) est une des manières les plus anciennes et les plus simples de faire du routage dynamique. Toutes les 30 secondes, chaque routeur envoie à tous ses voisins le contenu de sa table de routage. Lorsqu'un routeur reçoit une ligne de la table de routage de son voisin dont la destination n'est pas incluse dans sa propre table, il l'ajoute à sa table en indiquant comme interface, celle le connectant avec ce voisin. De plus lorsqu'un routeur que son voisin dispose d'un chemin plus court pour atteindre une destination, reçoit une ligne de la table de routage de son voisin dont la destination est incluse dans sa table, il modifie sa table de routage pour faire passer par ce voisin les messages pour cette destination.

Exercice 3

La table de routage d'un routeur 1 contient les lignes suivantes :

Destinataire	Interface	Distance
114.2.1.1	A	1
12.251.x.x	B	2
12.25.x.x	C	1
87.33.x.x	C	8
…	…	…

Ce routeur reçoit de son voisin, le routeur 2 sur l'interface B une table contenant les lignes suivantes (les interfaces ne sont pas indiquées) :

Destinataire	Interface	Distance
12.251.x.x	-	1
12.252.x.x	-	3
87.33.x.x	-	5
…	…	…

Comment le routeur 1 peut-il compléter sa table de routage avec les informations reçue par son voisin ?

Solution 3

Il peut ajouter la lignes suivante :

Destinataire	Interface	Distance
12.252.x.x	B	4

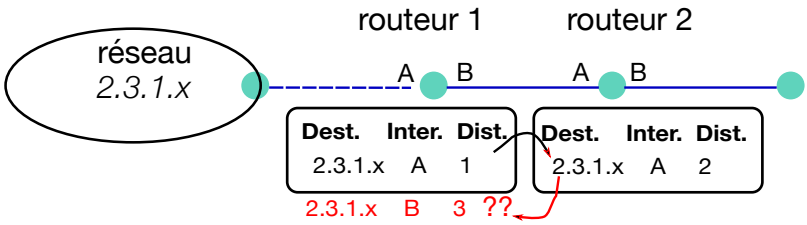
En effet, c'est une nouvelle destination que le routeur 1 peut maintenant joindre en transmettant les paquets au routeur 2 (sur l'interface B) qui saura les transmettre dans la bonne direction.

Le routeur 1 peut aussi modifier la ligne pour la destination 87.33.x.x en mettant

Destinataire	Interface	Distance
87.33.x.x	B	6

Cette destination déjà existance pour le routeur 1, mais elle peut être transmise plus rapidement en passant par le routeur 2 sur l'interface B (en 5+1=6 étapes) que par l'interface C (en 8 étapes)

Toutefois, si l'on applique cette méthode telle quelle, cela peut créer des situations où des erreurs dans les tables de routage se propagent à travers le réseau. Considérons par exemple le bout de réseau suivant :



Lorsque la connexion en traitillés fonctionne, le routeur 1 remplit sa table de routage et la transmet au routeur 2. Les tables de routage de ces routeurs contiennent donc les lignes indiquées en noir dans la figure. Si la connexion en traitillé se rompt, le routeur 2, va effacer de sa table de routage la ligne concernant la destination `2.3.1.x`, mais il serait tenté d'ajouter la ligne en rouge lorsqu'il recevra la table du routeur 2, ce qui serait erroné.

C'est pour éviter ces problèmes que la protocole RIP applique un certains nombre de principes, appliqués également par d'autres protocoles de routage.

1. Ne pas transmettre à une interface une information déjà reçue par cette interface. Ainsi, dans le l'exemple ci-dessus, selon ce principe, le routeur 2 ne pourra pas transmettre sa ligne au routeur 1, car cette information lui vient du routeur 1. C'est le principe de l'*horizon séparé* (*split horizon*).
2. Si une route est bouchée, transmettre cette information aux voisins. Dans le protocole RIP on indique ceci par une distance égale à 16. Toute destination à distance supérieure à 15 est considérée comme inaccessible. Dans l'exemple si dessus, le routeur 1 remplacera simplement la distance par 16 (au lieu de 1) et transmettra cette information au routeur 2 qui mettra à jour sa table de routage. C'est le principe de l'*empoisonnement de route* (*route poisoning*).

Ai-je compris ? – L'exemple d'Alice

Les paquets IP échangés entre le téléphone d'Alice et le serveur sont acheminé de routeur en routeur. Chaque routeur consulte sa table de routage pour savoir dans quelle direction transférer le paquet reçu. Ces tables de routage se constituent automatiquement en échangeant des informations avec les routeurs voisins.

1.4 World Wide Web

Le **World Wide Web** (WWW), littéralement la « toile (d'araignée) mondiale », est un système qui permet de consulter avec un navigateur, à travers l'Internet, des pages accessibles sur des sites.

1.4.1 Historique

Pendant ses premières décennies (jusque dans les années 90), seuls les universitaires, les militaires, certaines entreprises et une communauté d'enthousiastes (largement issue du mouvement hippie) utilisaient Internet. Les utilisations principales étaient la discussion écrite (le *chat* dans un terminal), la connexion sur un ordinateur à distance, l'email et le transfert de fichiers entre ordinateurs.

Pour aller chercher un fichier se trouvant sur un autre ordinateur, il fallait savoir exactement sur quelle machine celui-ci se trouvait et où il se situait dans cette machine. Il fallait donc établir des listes de ressources et de leur location dont la maintenance et l'utilisation étaient fastidieuses.

C'est en voulant résoudre ce problème que Tim Berners-Lee, un scientifique anglais du Conseil Européen de la Recherche Nucléaire (CERN) à Genève, a développé les technologies du Web entre 1989 et 1991. Celles-ci se sont rapidement développées après que le CERN les ait gratuitement mises à disposition du public. Des centres de recherche, universités, entreprises (d'informatique et de média) et d'autres organisations ont créé leur site web afin de pouvoir facilement diffuser des informations par ce canal. Ceci offrait un usage supplémentaire de l'ordinateur dont les foyers se sont équipés massivement, diffusant ainsi l'accès à Internet au sein de la population américaine et européenne.

1.4.2 Les technologies du Web

Le web repose sur trois technologies mises ensemble et qui permettent de naviguer dans une "toile" de documents. La première, l'URL, spécifie un format permettant de spécifier la localisation d'un document. La seconde, le protocole HTTP, permet de demander et de recevoir un document identifié par son URL. La troisième, le langage HTML, permet de décrire le contenu d'un document (une page web) pouvant contenir des liens vers d'autres documents spécifiés par leur URL.

Ces trois technologies sont rassemblées dans un *navigateur web*, un programme qui permet de

1. spécifier une page web à visiter en indiquant son URL, typiquement dans une barre de navigation
2. demander la page web au serveur correspondant et la réceptionner en utilisant le protocole HTTP
3. afficher le contenu de la page web (décrite au format HTML), y compris les liens cliquables permettant d'afficher d'autres pages web.

Document historique

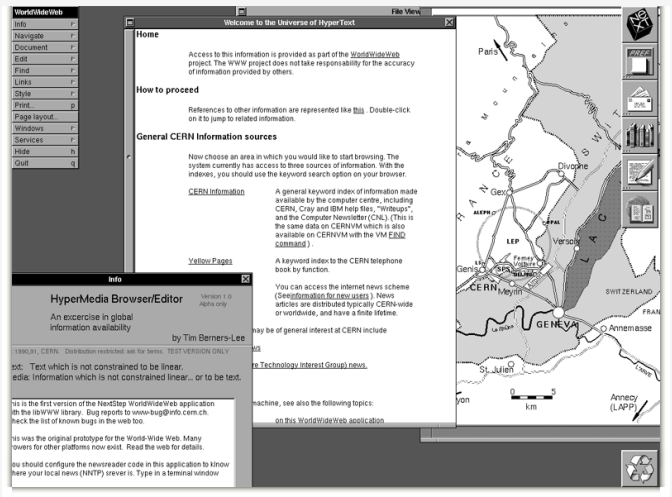


Fig. 1.7 – Un des premiers navigateurs web développé par Tim Berners-Lee. Les images s'affichaient sur des fenêtres séparées.

URL

L'URL (*Uniform Resource Locator*) est une manière de spécifier la localisation d'un document disponible sur Internet. Un exemple d'URL peut être par exemple "https ://www.champignons.ch/fichiers/fr/contact.html".

Une URL comporte trop parties, qui sont les suivantes dans notre exemple |https| ://www.champignons.ch|/fichiers/fr/contact.html|. Autrement dit, une URL se compose généralement de la manière suivante :

protocol :*hôte*/*chemin*

1. Le *protocole*, dans notre exemple `https`, indique le protocole utilisé pour avoir accès à la ressource. Pour le web, ce protocole est toujours `http` ou `https`, sa version sécurisée. Mais l'URL étant aussi utilisée en dehors du web, il y a d'autres protocoles possibles, par exemple `ftp` pour faire du transfert de fichier.
2. L'*hôte* spécifie la machine (ou le serveur) où aller chercher le fichier. Cela peut être un nom de domaine, mais également une adresse IP
3. Le *chemin* indique quel fichier on souhaite obtenir de la part du serveur. On part de la racine "/" (connue du serveur) et on descend dans l'arborescence selon les répertoires indiqués. Par exemple `/fichiers/fr/contact.html` est le fichier `contact.html` qui se trouve dans le répertoire `fr` qui se trouve lui-même dans le répertoire `fichiers`.

Dans le protocole HTTP, si le chemin est un répertoire (et pas un fichier), le fichier par défaut `index.html` présent dans ce répertoire est envoyé par le serveur.

HTTP

HTTP (acronyme de HyperText Transfer Protocol) est le protocole qui régit la manière dont un client web (par exemple le navigateur web de Alice) et un serveur web (par exemple le site www.champignons.ch) vont interagir l'un avec l'autre.

Par exemple si le client demande au serveur de lui envoyer la page web `accueil.html`, il lui enverra requête GET suivante :

```
GET accueil.html HTTP/1.1
```

ce qui signifie "envoie-moi la page accueil.html avec la version 1.1 du protocole HTTP". S'il trouve la page en question, le serveur pourra alors envoyer la réponse suivante :

`HTTP/1.1 200 OK` suivie de diverses informations ainsi que la page web demandée. Le code `200 OK` indique que la requête peut être honorée.

Si la page `accueil.html` n'existe pas, alors le serveur pourra l'indiquer au client en envoyant la réponse suivante :

```
HTTP/1.1 404 Not Found
```

Le navigateur web pourra alors afficher l'"erreur 404" au pour l'utilisateur.

Fig. 1.8 – Le serveur retourne un message d'erreur s'affiche lorsqu'on demande une page qui n'existe pas.

Il y a d'autres sortes de requêtes que le client peut envoyer au serveur, par exemple `POST` pour envoyer une information du client au serveur, utilisé par exemple lorsqu'on remplit un formulaire en ligne.

Si un utilisateur utilise le protocole HTTP pour surfer sur le web, une tierce personne qui a accès au trafic sur Internet peut savoir quelle page web a été visitée par cet utilisateur et ce que le serveur lui a envoyé comme information (par exemple des messages privés). C'est pourquoi on utilise généralement plutôt le protocole HTTPS qui encrypte les requêtes et réponses HTTP. Ainsi un observateur peut toujours savoir avec quel site on communique lorsqu'on surfe sur le web en regardant l'entête IP, mais ne pourra pas connaître les détails des pages demandées et transmises.

HTML

HTML (HyperText Markup Language) est un langage de description des pages web. Il permet de spécifier le contenu et l'apparence d'une page web afin que le navigateur web puisse l'afficher. Supposons par exemple que le site www.champignons.ch envoie à Alice une page web contenant le nom d'un champignon ainsi qu'une photo de celui-ci. Une manière de décrire cette page avec le langage HTML serait la suivante :

```
<html>
<body>
 <h1 style="color:red"> L'amanite tue-mouche </h1>
 <p> L'amanite tue-mouche est très belle mais très dangereuse ! </p>
 <img src="photo.jpg" height="250" />
</body>
</html>
```

Les éléments de cette page sont indiqués par des *balises* indiquées par des crochets pointus (<>) et peuvent être imbriqués les uns dans les autres. Ainsi la page (entre `<body>` et `</body>`) contient un titre (entre `<h1>` et `</h1>`) de couleur rouge, un paragraphe de texte (entre `<p>` et `</p>`) ainsi qu'une image (`<img>`) disponible dans le fichier `photo.jpg` et de hauteur 250 pixels. Cette page pourra ainsi être affichée de la manière suivante dans le navigateur web.

La plupart des navigateurs web permettent de visualiser le *code HTML* des pages visitées. Un aspect important de la création de sites web consiste à écrire du code HTML qui sera mis sur le serveur pour être transmis au visiteur du site web. Cela peut se faire en écrivant directement du code HTML dans un fichier texte, ou à l'aide d'un outil de création de sites web qui se charge d'écrire le code HTML selon les indications données par la personne concevant le site.

1.4.3 Les évolutions du Web

Javascript

Dans la version originale d'HTML, les moyens d'interagir avec une page web étaient très limités, par exemple cliquer sur les liens que la page proposait. Les personnes utilisant et développant le web ont vite voulu enrichir l'interactivité. C'est pourquoi, en 1995, les développeurs de Netscape, le navigateur web populaire de l'époque, ont ajouté la possibilité d'intégrer des programmes dans les pages web. Ils ont pour ceci inventé un langage de programmation, javascript, qui puisse être interprété et exécuté par le

navigateur web. Cela permettait d'avoir une page web avec du contenu dynamique qui réagisse aux actions des personnes utilisatrices, par exemple pour changer la langue du texte lorsque on appuie sur un petit drapeau. Cela permet aussi de programmer des animations sur une page web.

Le Web dynamique

Au début, les pages web étaient des fichiers HTML stockés sur les serveurs. C'est ce qu'on appelle le web *statique*. Si les sites web statiques existent toujours, par exemple modulo-info.ch, beaucoup de sites web sont dynamiques, c'est-à-dire que le fichier HTML est généré par le site au moment où la requête est faite. Cela permet de servir une page différente selon l'utilisateur ou selon les arguments de la requête qui sont des indications supplémentaires ajoutée à la requête après l'URL après les le signe ?.

Micro-activité

Effectuer une recherche sur un navigateur web et consulter la barre de navigation. Quels sont les arguments de votre requête et pouvez-vous en comprendre la signification ?

Exercice 1

Parmi les sites web suivants, lesquels ont besoin d'être dynamiques et lesquels peuvent se contenter de fournir un contenu statique ?

1. Un site d'achats en ligne
2. Un site indiquant les horaires d'ouverture et de fermeture d'un magasin.
3. Un site de consultation du catalogue d'une bibliothèque
4. Un site de présentation d'une entreprise
5. Un site avec les documents d'un cours universitaire ou scolaire
6. Un site d'e-banking

Pour les sites qui peuvent être statiques, quelles possibilités supplémentaires pourraient être offertes par un site dynamique ?

Le Web 2.0

Le web 2.0 fait référence à la tendance, initiée au débit des années 2000, de proposer des pages web permettant aux internautes de contribuer du contenu, et pas uniquement de lire des fichiers comme c'était le cas jusqu'alors. Les blogs, forums, wikis, et les réseaux sociaux font partie de ce développement qui voit exploser l'aspect participatif du web. Ce n'est en effet plus nécessaire de connaître la syntaxe HTML et d'avoir son propre serveur pour mettre du contenu à disposition des internautes de la planète. Si les développements techniques qui ont permis le web 2.0, étaient peu importants, ils ont eu un effet considérable sur la manière dont la population s'est approprié le web pour en faire un espace d'expression et de partage duquel ont émergé des réseaux sociaux d'aujourd'hui.

Ai-je compris ? – L'exemple d'Alice

Pour demander la page web du site *champigons.ch* le navigateur web d'Alice va utiliser le protocole HTTP (ou HTTPS) qui spécifie des mots de code indiquant qu'on veut accéder à une page donnée ou envoyer des informations au serveur. Le serveur va répondre avec le même protocole pour envoyer la page ou un message d'erreur si ce n'est pas possible. La page, elle-même, est envoyée au format HTML, c'est à dire sous forme de texet et d'images. Le navigateur va lire ce texte qui va lui indiquer ce qu'il faut afficher pour Alice.

1.5 Interopérabilité

Si Internet a connu un développement aussi remarquable, c'est aussi grâce à certains choix techniques et de gouvernance qui ont permis de le rendre accessible relativement facilement. Des personnes, organisations et entreprises pouvaient ainsi participer à sa construction et son développement.

Certains de ces choix sont décrits ci-dessous.

1.5.1 Un modèle en couches

La communication sur Internet se fait selon une pile de protocoles qui s'ajoutent les uns aux autres tout en étant indépendant les uns par rapport aux autres selon un *modèle en couches*. Ainsi, le protocole HTTP est responsable de l'échange de pages web, mais toute la partie s'assurant du bon transfert et de la bonne réception des paquets est gérée par le protocole TCP. Mais ce protocole repose sur le protocole IP pour l'envoi des paquets indidivduels qui lui-même repose sur différents protocoles selon que les paquets circulent par le wifi, un câble sous-marin, la 4G ou de la fibre optique. Ainsi les niveaux supérieurs peuvent s'abstraire des niveaux inférieurs, et vice-versa. Si un nouveau support physique de communication est inventé (par exemple la téléportation quantique), il suffit de développer un protocole de communication propre à ce support et on pourra utiliser le protocole IP pour la transmission de paquets, ce qui permettra à ce nouveau support de s'intégrer sans difficulté à Internet.

On a ainsi défini le modèle de la Fig. 1.9 en 4 "couches" de protocoles : la première couche "liaison réseau" définit comment les données sont transmises entre deux appareils directement connectés ou du même réseau local. Le protocole en question dépend donc du type de connexion entre les deux appareils (wifi, câble électrique, fibre optique, etc.). La deuxième couche, "Internet", définit comment les données sont transmises entre deux machines du réseau, c'est le protocole IP vu précédemment. La troisième couche "transport" définit comment les données sont segmentées (c'est-à-dire découpée et morceaux) et envoyées par l'émetteur et reconstituées et quittancées par le récepteur, c'est le protocole TCP également vu précédemment. La quatrième couche est la couche applicative qui définit comment deux applications (ou programmes) communiquent entre elles, par exemple le protocole HTTP qui détermine la communication entre un navigateur web et un serveur web. D'autres exemples figurant dans cette couche pourraient inclure la manière dont l'application TikTok d'un smartphone communique avec le serveur de TikTok.

Ainsi, lorsque le navigateur web d'Alice demande une page au serveur web, ces deux applications (le navigateur et le serveur) sont en communication en utilisant le protocole HTML. Pour transmettre la requête HTML d'Alice, une connexion entre Alice et le serveur web sera établie en utilisant le procole TCP. Au besoin, ce protocole découpera la requête ou la page web en petits morceaux et ajoutera les entêtes TCP à chaque morceau, qui sera envoyé individuellement en utilisant le protocole IP (en ajoutant y donc l'entête IP). Selon le type de connexion, (4G, wifi, cable), les paquets IP seront transmis selon différents protocoles à des routeurs qui les achemineront jusqu'au destinataire qui réassemblera les paquets selon le protocole TCP et fournira la requête HTML d'Alice au serveur web ou la page web demandés au navigateur d'Alice.

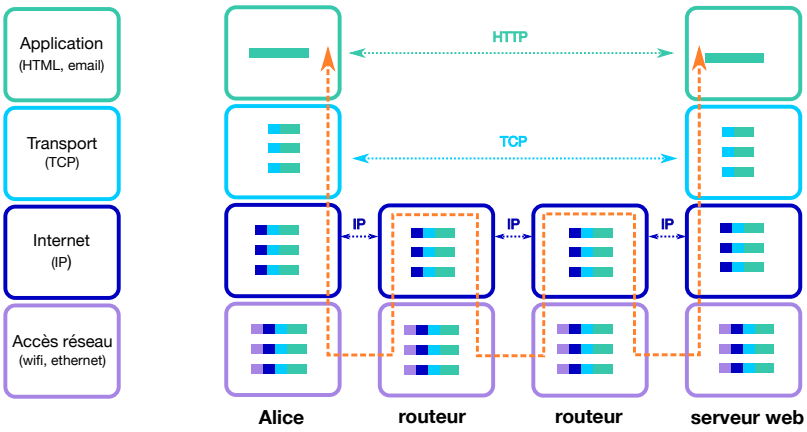


Fig. 1.9 – Gauche : le modèle en 4 couches de la communication par Internet. Droite : Exemple de l'application de ce modèle à la communication entre le navigateur web d'Alice et un serveur web. Lorsque les applications veulent s'échanger de l'information, cet échange se fait selon un protocle de la couche "Application" par exemple HTTP. La requête ou la page web ainsi formées (représentés par le rectangle vert) sont ensuite traitées par le protcole TCP de la couche "Transport" qui va découper ces données en petits paquets, y ajouter une entête TCP numérotée (en bleu ciel) et envoyés à leur destinataire par le protocole IP de la couche "Internet". Avec ce protocole, une seconde entête (représentées en bleu foncé) est ajoutée à chaque paquet qui est envoyé sur le réseau par un protocole propre au type de réseau utilisé (en y ajoutant encore une entête mauve). L'information ne passera d'habitude pas directement d' Alice au serveur web, mais par des routeurs qui achemineront les paquets IP jusqu'à leur destination, en utilisant les différents protocoles de la couche d'accès réseau selon les besoins.

Ce modèle en 4 couches a été ensuite développé en un modèle en 7 couches appelé OSI (pour *Open System Interconnection*). Dans ce modèle, la couche d'accès réseau est séparée en deux couches, la couche physique qui décrit comment le signal est codé dans un médium donné (fibre optique, onde électromagnétique, etc.) et la couche de liaison qui indique comment un groupe de bits (appelé une trame) est envoyé au sein un réseau local (par exemple le wifi, ou un réseau ethernet). Ce modèle ajoute deux couches à la couche "Application", la couche de présentation qui spécifique comment les données sont encodées (par exemple avec la table ASCII) et potentiellement encryptées, et la couche "Session" qui gère les questions d'authentification et d'autorisation, par exemple lorsque vous vous connectez à un service payant sur le web.

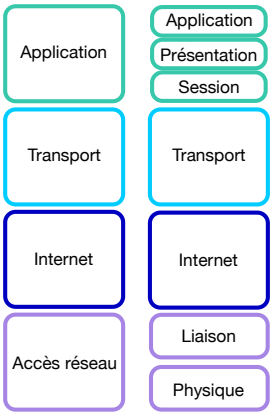


Fig. 1.10 – Le modèle (TCP-IP) en quatre couches et, à sa droite, le modèle OSI en sept couches. La couche "Application" a été séparée en trois couches, et la couches "Accès réseau" a été séparée en deux couches.

Le modèle OSI indique la manière dont les choses devraient se passer pour garantir à la fois la sécurité et la modularité des communications, mais il n'est dans la pratique pas toujours entièrement respecté, en particulier pour les couches supérieures.

1.5.2 Des protocoles ouverts

Les protocoles décrits ci-dessus ont été établis sur proposition de différentes personnes travaillant principalement dans les universités ou les entreprises de télécommunication et adoptés par consensus après beaucoup de discussion. L'idée principale étant qu'Internet n'appartient à personne et qu'il s'agit d'une oeuvre collective à laquelle toute personne dotée des compétences nécessaires peut contribuer. Ces protocoles sont *ouverts* dans le sens que chacun peut y avoir accès et les implémenter à sa manière. Par exemple, quelqu'un qui souhaiterait développer un routeur peut avoir accès à toutes les informations nécessaires pour le faire.

La collaboration autour de la définition des protocoles d'Internet est structurée autour l'Internet Society, une association à but non lucratif dont le but est le développement d'Internet. L'Internet Engineering Task Force et un groupe de personnes qui discutent des aspects techniques d'Internet. Ce groupe est (théoriquement) ouvert à toute personne qui souhaite s'y impliquer. Les discussions s'articulent autour de "Requests For Comments" (RFC) qui sont des documents publics qui proposent des idées qui sont discutées, et, pour certaines d'entre elles, adoptées par consensus. Le premier RFC, RFC1 a été formulé en 1969 pour proposer un protocole de communication sur ARPANET, le projet de recherche militaire américain qui a donné naissance à Internet. Toutes les technologies d'Internet décrites ci-dessus ont été proposées par le biais de RFC, par exemple IPv4, RIP, HTML, etc.

Micro-activité

Chercher et lire le RFC 8962, en particulier l'abstract et les parties 7 et 8, ainsi que la date. De quoi s'agit-il ?

1.5.3 La neutralité d'Internet

Un des principes fondateurs d'internet est sa *neutralité*. Cela signifie que les paquets IP sont acheminés vers leur destination sans discrimination de source, de destination ou de contenu. Contrairement à la poste suisse, où certains courriers (par exemple le courrier A) sont prioritaires par rapport à d'autres, les paquets IP sont tous logés à la même enseigne sur Internet. Cela permet d'éviter que certains services (par exemple un site web) puissent payer plus cher pour que ses paquets arrivent plus rapidement chez leurs destinataires et offrir ainsi un service plus rapide au détriment d'autres services. Certains acteurs, tels que les fournisseurs d'accès à Internet se sont opposés à la neutralité du net, car cela leur aurait permis de mettre leurs clients en concurrence sur les débits fournis et ainsi augmenter leurs tarifs et donc leurs bénéfices. Ou alors, il leur serait possible de privilégier l'acheminement des paquets liés à leurs propres services (par exemple Swisscom, pourrait privilégier l'acheminement des paquets liés à son service de télévision au détriment d'autres chaînes.)

Le respect de la neutralité d'Internet est différent de pays en pays, certains, comme la Suisse l'ayant inscrite dans la loi.

Micro-activité

Lire l'article 12e [5] de la loi fédérale sur les télécommunications qui concerne la neutralité d'Internet. Quel alinéa garantit la neutralité du réseau ? Cette garantie est-elle absolue ?

5. https://www.fedlex.admin.ch/eli/cc/1997/2187_2187_2187/fr#art_12_e

1.5.4 L'universalité d'Internet en question

Avec la montée en puissance des entreprises privées, une partie de l'ouverture qui caractérisait les débuts d'Internet est remise en question. Ainsi, les entreprises qui ont développé les réseaux sociaux l'ont fait en utilisant des protocoles fermés (ou privés). Par exemple, le protocole par lequel l'application Whatsapp communique avec le serveur est gardé secret. Ceci permet d'empêcher que d'autres personnes ne développent des applications compatibles avec Whatsapp et y fassent ainsi concurrence. Pour illustrer la différence avec un protocole ouvert (ou public), on peut comparer Whatsapp (protocole fermé) avec l'email qui repose sur un protocole ouvert (SMTP). Le fait que le protocole de l'email soit public permet à toute personne qui en a les capacités d'offrir un service d'email. (Certaines personnes installent ainsi leur propre serveur email hébergé sur leur ordinateur.) Tous ces services d'email différents, qui peuvent être commerciaux, privés, ou artisanaux, sont compatibles les uns avec les autres, car ils suivent le même protocole SMTP. Ceci est très différent de Whatsapp qui ne peut être utilisé qu'avec l'application Whatsapp et donc tous les messages Whatsapp sont centralisés chez une seule entreprise. On observe certaines tentatives de créer des réseaux sociaux sur des protocoles ouverts, par exemple Mastodon pour le microblogging, PeerTube pour la vidéo, ou diaspora, mais leur succès reste limité, notamment car elles n'ont pas les ressources financières qui leur permettraient de rivaliser avec leurs concurrentes à visée lucrative.

Une autre tendance qui remet en question la décentralité d'Internet est le développement du cloud. Avec les services de cloud, les documents, les données et les sites web se concentrent dans les serveurs des entreprises offrant ces services. Ainsi, si une panne affecte un de ces services offerts par Google ou Microsoft, ou si la sécurité d'un tel service est compromise, les répercussions seront globales.

Enfin, si Internet donnait à ses débuts une impression d'universalité, on s'est rendu compte que l'utilisation des caractères ASCII, la syntaxe de HTML et de l'URL étaient peu propices aux alphabets non latins, et qui ne s'écrivent pas de gauche à droite. Tout choix "technique" est ancré dans un contexte social et culturel duquel il est difficile de faire abstraction. Des inititatives pour rendre Internet plus universel ont été prises, comme le fait de pouvoir entrer des URL en caractères chinois. Il n'en reste pas moins que les structures qui gèrent Internet restent des entités de droit américain, et que l'occident garde une place prépondérante dans le façonnage d'Internet. Certains états plus autoritaires, tels que la Chine ou la Russie, souhaitent avoir un contrôle plus strict de ce que leur population font sur Internet et tentent de filtrer certains contenus. A terme, il n'est pas exclu que se développent plusieur réseaux en parallèle avec des politiques d'ouverture très différentes.

1.6 Conclusion

En quelques décennies, Internet est passé d'un moyen de communication et d'échange utilsés par des communautés relativement restreintes issues du monde académique, des mouvements hippies, et autres enthousiastes à une infrastructure essentielle de notre organisation sociale et économique. Cette évolution, rendue possible par le caractère ouvert et non hiérarchique d'Internet, a fait émerger de nouveaux acteurs économiques, politiques, ou criminels qui tirent profit de la dépendance de nos sociétés à cette infrastructures. Ainsi, conçu initialement comme un outil de résilience, Internet et peut-être en train de devenir également un point de vulnérabilité de nos modes de vie. Avec la multiplication des cyberattaques, les tentatives de manipulation de masse à travers les réseaux sociaux, les principes d'ouverture et de bonne foi qui ont guidés le développement initial d'Internet sont mis à mal. La notion de cybersécurité, prend une importance grandissante, que ce soit contre le vol de données, le vol d'identité, les logiciels de rançons, ou les attaques de serveurs.

Dans l'Union Européenne, le Réglement général sur la protection des données (RGPD), entré en vigueur en 2018, définit ainsi toute une série de principes que les entreprises et organismes doivent respecter afin de garantir la protection des données personnelles. Ces principes incluent par exemple le droit de savoir qui détient quelles données sur nous, le droit d'obtenir la correction des données erronées ou leur effacement, l'obligation pour les sites web d'obtenir le consentement des usagers concernant l'utilisation de leurs données des cookies, ainsi que l'obligation d'informer les autorités et les personnes touchées en cas de fuites de données, par exemple lors d'une cyberattaque.

Micro-activité – Le Réglement général sur la protection des données (RGPD)

Aller sur le site https://www.cnil.fr/fr/reglement-europeen-protection-donnees/ et regarder le sommaire.

1. Combien d'articles ce réglement contient-il ?
2. Lire l'article 5 et résumer les grand principes de ce réglement.

Ai-je compris ?

1. Je sais comment est structuré Internet.
2. Je sais ce qu'est une adresse IP et un nom de domaine et à quoi cela sert.
3. Je sais ce qu'est un protocole et à quoi cela peut servir.
4. Je sais à quoi sert un entête IP et le protocole TCP.
5. Je sais à quoi sert un routeur.
6. Je sais à quoi sert une table de routage et quelle information elle contient.
7. Je sais comment un routeur peut dynamiquement une table de routage.
8. Je comprends la différence entre Internet et le Web.
9. Je connais les trois technologies du Web et comment un navigateur web les utilise.
10. Je comprends le principes des couches de protocoles.
11. Je comprends la différence entre un protocole ouvert (public) et fermé (privé) et quels en sont les enjeux pour Internet