Chapter 1

Protocoles réseau

Le réseau militaire Arpanet né 1958 au Etats-Unis a engendré le réseau mondial Internet. Au début des années 1960 nait l'idée de découper l'information en paquets indépendants connaissant l'adresse du destinataire. Ils peuvent ainsi emprunter des routes différentes de routeur en routeur. Ces routeurs sont des ordinateurs assurant le routage des paquets. L'information est finalement reconstituée chez le destinataire.

10 ans plus tard naît le protocole IP: chaque ordinateur a une adresse numérique codée sur 4 octets. Associé au protocole TCP pour le transport des données émerge le protocole TCP/IP vers 1974. Le modèle OSI est un modèle théorique des réseaux sur lequel se calque le protocole TCP/IP mais sans correspondance exacte.

Lorsqu'une machine se connecte à internet, elle doit respecter ces normes ou protocoles expliqués ici dans leurs grandes lignes.

1.1 Modèle en couches

Le modèle OSI (Open System Interconnexion) a été créé en 1977 afin d'éviter que chaque fournisseur réseaux et systèmes n'utilise sa propre solution. Ce principe, volontairement imprécis par rapport aux réalités techniques, est utilisé pour acheminer des données d'une machine à l'autre. Il est organisé en 7 couches.

Le modèle TCP/IP, réellement utilisé, s'inspire dans le principe et sur certaines couches du modèle OSI. Voici une comparaison de ces deux modèles:

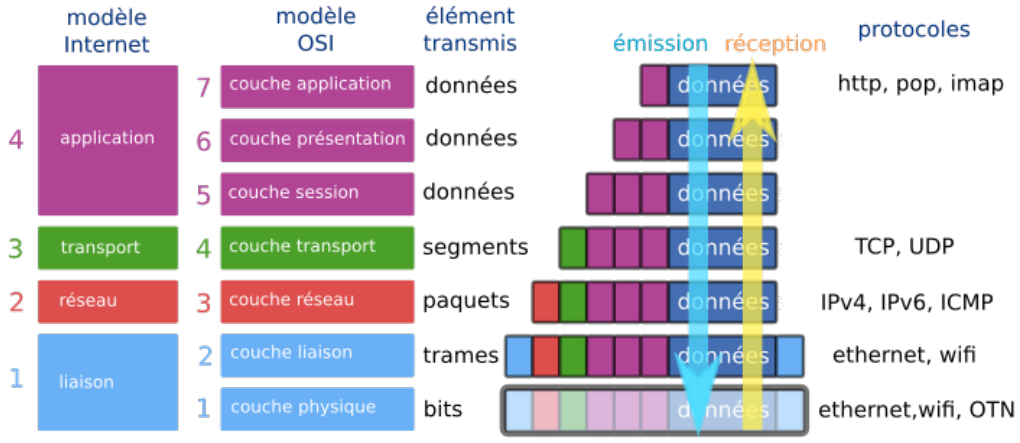


Figure 1.1: Modèle OSI et TCP/IP

Le protocole **IP a pour but l'adressage des machines sur le réseau ainsi que le routage des paquets.** Le protocole **TCP** s'appuie sur IP pour permettre l'envoi de messages de longueur

arbitraire et **garantit à l'expéditeur que le destinataire a bien reçu les paquets**. TCP numérote les paquets pour permettre leur réassemblage chez le destinataire, il vérifie en outre leur intégrité en vérifiant que les données ne soient pas altérées entre deux routeurs.

Exemple : Le logiciel *Wireshark* est un analyseur de paquets, il peut enregistrer les données transitant par le biais d'un réseau local et permet de capturer chaque paquet du flux de données traversant le réseau. On demande une page Web par un navigateur. Voici une capture d'écran où la structure des couches apparait:

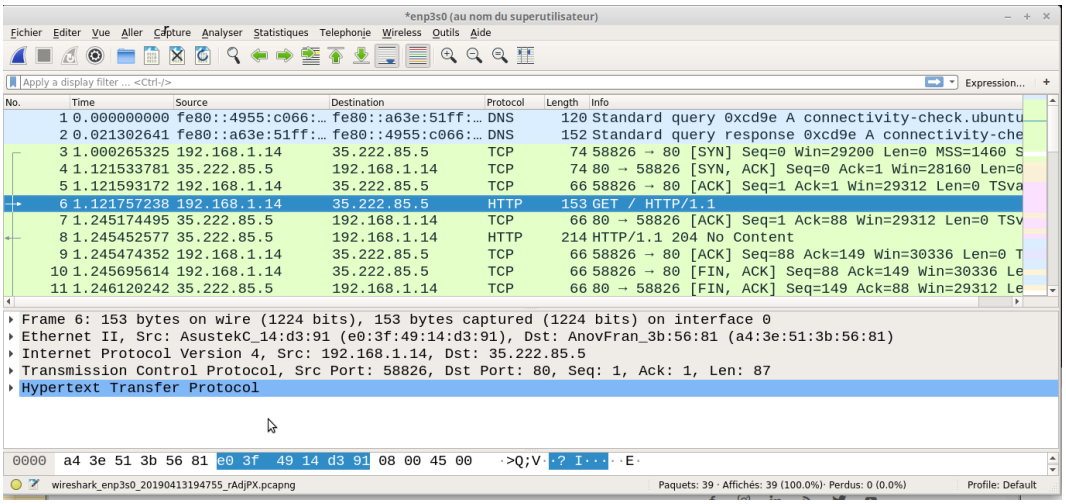


Figure 1.2: Les couches analysées avec Wireshark

La ligne 6 sélectionnée est une requête HTTP utilisant la méthode GET. On peut voir sur la fenêtre du bas les quatre couches du modèle TCP/IP:

- Ethernet (accès au réseau) les adresses MAC des cartes réseau sont visibles. e0:3f:49:14:d3:91 pour la source.
- IP (réseau) : les adresses source (192.168.1.14, carte réseau) et destination 35.222.85.5 .
- TCP (transport).
- HTTP (application).

Lors de la demande de cette page Web, l'ordre d'utilisation des protocoles est le suivant:

n° TCP/IP	n° OSI	Nom	Exemple de protocole
4	5, 6, 7	Application	HTTP, POP, IMAP
3	4	Transport	TCP, UDP
2	3	Réseau	IPv4, IPv6, ICMP
1	1, 2	Liaison	Ethernet, Wi-Fi

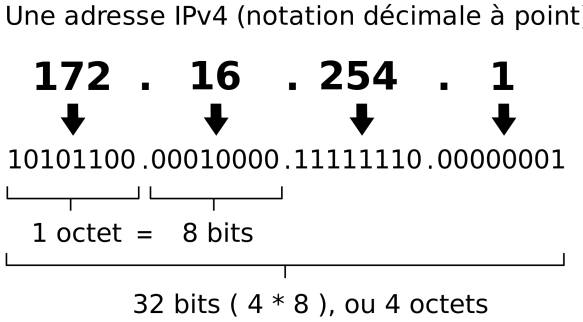
Figure 1.3: En bleu, la suite de protocole utilisée en 1.2

Quand un client se connecte au serveur, il a besoin du nom d'hôte (par exemple, `Lilo.org`) et d'un numéro de port, ici le navigateur tente d'accéder à un site en *http*, le port est généralement 80. En *https*, c'est 443. Le protocole DNS se charge de convertir l'adresse symbolique `Lilo.org` en adresse IP. Les serveurs DNS sont en quelque sorte l'annuaire d' internet.

1.2 Des adresses

Pour identifier une machine sur un réseau désormais planétaire, il faut distinguer différents types d'adresse.

- Le protocole IP assure l'adressage des machines sur le réseau et le routage des paquets. L'adresse IP ou *internet protocol* qui correspond grossièrement à l'adresse postale de la machine. Cette adresse est codée sur 4 octets en IPV4 soit 2^{32} possibilités. Chaque octet contient des nombres compris entre 0 et 255. L'adresse **127.0.0.1** est réservé au *localhost* (*hôte local*), interface virtuelle correspondant à la machine où on se trouve.



  Une adresse IPv6 est longue de 128 bits et se compose de huit champs de 16 bits, chacun étant délimité par deux-points (:). Chaque champ doit contenir un nombre hexadécimal, à la différence de la notation en format décimal avec points des adresses IPv4. Dans l'illustration suivante, les x représentent des nombres hexadécimaux.

  Exemple: 2a01:e0a:222:b600:ec2e:d045:c908:c4d5/64

- L'adresse MAC ou adresse physique qui permet d'identifier de façon unique une carte réseau sur une machine: chaque adresse MAC va être unique au monde. Cette adresse est codée sur 6 octet soit 2^{48} ou 256 mille milliards de possibilités .

  Exemple En 1.1, l'adresse MAC d'une carte ethernet a été récupérée avec l'analyseur de réseau *Wireshark*. (voir aussi 1.3.1).

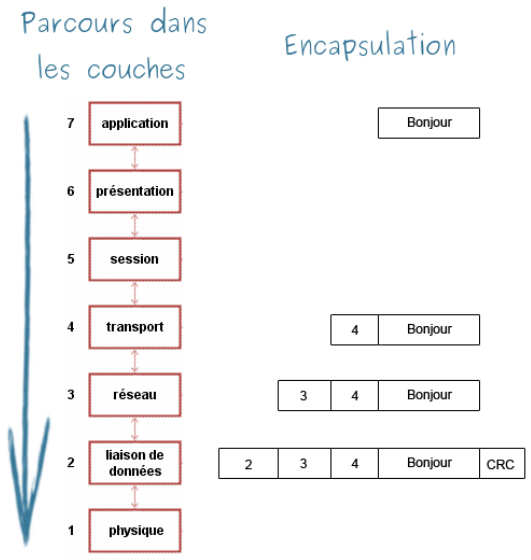
  Notons qu'un switch Ethernet qui relie p̂hysiquement plusieurs machines analyse la trame à distribuer. Lors d'un branchement d'un nouvel ordinateur sur le switch, celui-ci récupère son adresse MAC, ce qui lui permet de trier les messages et de ne les distribuer qu'au bon destinataire.

- Le port est l'adresse d'une application sur une machine. Comme souligné en **1.1**, en *http* le port est généralement 80 et 443 en *https*. On sépare l'adresse IP ou symbolique par deux points pour spécifier le port.

  Exemple `http://maths-code.fr:80` se connecte sur le port 80, ce qui est fait par défaut pour le protocole http.

Pour faire communiquer des machines différentes, avec des systèmes d'exploitations différents, il est nécessaire d'utiliser un protocole: les protocoles réseau fédèrent les réseaux locaux de proche en proche via les routeurs. C'est pour cela que trouver le chemin s'appelle le *routage*. Le protocole **IP** est le plus utilisé: chaque machine a une adresse IP affecté de manière non durable, contrairement à l'adresse MAC qui identifie le matériel réseau de façon définitive.

1.3 Encapsulation des données



Encapsulation Chez l'expéditeur, au fur et à mesure de la descente dans les couches, des informations sont ajoutées en entêtes des données à envoyer: adresse IP source et destination, adresse MAC des machines, etc. Ce procédé s'appelle l'encapsulation. Le bloc informations+données représentépar les rectangles non détaillés ci-contre deient au fur et à mesure de l'encapsulation::

- La **trame Ethernet**, couche 1 et 2 (le CRC est une clé de contrôle des erreurs).
- Le **datagramme IP**, couche 3.
- Le **Segment TCP** (ou datagramme UDP), couche 4.

Chez le destinataire, le message remonte les couches du modèle OSI et arrive à l'application sur la machine B.

1.3.1 Quelques commandes

Exemple 1: Dans un terminal, tapez `ip a` sous Linux ou `ifconfig` sous Window$. Vous obtenez une réponse du type:

```
 romain@Hal:~$ ip a
1: lo:
<LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever

2: enp3s0:
<BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether e0:3f:49:14:d3:91 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.49/24 brd 192.168.0.255 scope global dynamic noprefixroute enp3s0
       valid_lft 41736sec preferred_lft 41736sec
    inet6 2a01:e0a:222:b600:ec2e:d045:c908:c4d5/64 scope global dynamic noprefixroute
       valid_lft 86128sec preferred_lft 86128sec
    inet6 fe80::4955:c066:cae0:6a90/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

3: wlp5s2: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 5c:d9:98:09:c8:05 brd ff:ff:ff:ff:ff:ff
```

L'interface **lo** pour localhost, **enp** pour ethernet et **wlp** pour wifi. L'adresse IP de la carte réseau ethernet est 192.168.0.49

En IPV4, Les informations transportées sont successivement encapsulées quand elles passent d'une couche à la couche inférieure: cela signifie que l'on ajoute des informations au fur et à mesure de la descente dans ces couches. Ces informations transitent de routeur en routeur: ce sont des ordinateurs dont la fonction est d'acheminer des informations sur le réseau.

Exemple 2: La commande `ping` permet de tester qu'une machine distante est accessible depuis la nôtre.

```
wuuf@Hal:/$ ping education.gouv.fr
PING education.gouv.fr (185.75.143.24): 56 data bytes
64 bytes from 185.75.143.24: icmp_seq=0 ttl=50 time=12,650 ms
64 bytes from 185.75.143.24: icmp_seq=1 ttl=50 time=12,863 ms
64 bytes from 185.75.143.24: icmp_seq=2 ttl=50 time=12,069 ms
```

La machine à l'adresse education.gouv.fr est accessible depuis 185.75.143.24. Le paquet qu'elle a retourné a une durée de vie - **time to live ou ttl**- de 50 : c'est le nombre de routeur qu'il peut encore traverser avant d'être détruit, cela évite qu'un paquet tourne indéfiniment sur le réseau. Son temps de réponse est d'environ 12 ms.

`ping` utilise le protocole ICMP (Internet Control Message Protocol)

Exemple 3: La commande `traceroute` (Linux) ou `tracert` (Window$) permet de trouver l'itineraire suivi entre émetteur et destinataire.

```
 wuuf@Hal:/$ traceroute education.gouv.fr
traceroute to education.gouv.fr (185.75.143.24), 30 hops max, 60 byte packets
 1  _gateway (192.168.0.254)  0.214 ms  0.265 ms  0.309 ms
 2  194.149.169.89 (194.149.169.89)  8.684 ms  8.713 ms  8.727 ms
 3  * * *
 4  193.253.13.65 (193.253.13.65)  7.940 ms  8.708 ms  8.723 ms
 5  ae52-0.nridf201.Aubervilliers.francetelecom.net (193.252.98.233)  8.743 ms  8.779 ms
 6  ae41-0.nrlil101.Villeneuve-dascq.francetelecom.net (193.252.160.217)  14.923 ms  12.685 ms
 7 ***
 8 ***
```

La première ligne est naturellement la box internet: gateway ou passerelle. C'est le prmeier routeur rencontré. Celle-ci assure la connection avec le réseau internet en transformant les adresses privées en adresses publiques. La seconde ligne est l'adresse du premier routeur après la box auquel la ligne est rattachée. La ligne 6 indique le dernier routeur.

Exercice

1.4 Réseaux et masque de réseau

1.4.1 Classe IP

Reprenons l'adresse IP 172.254.1, celle-ci indique l'adresse de la machine en fournissant les indications d'adresse du réseau et des machines hôtes sur le réseau. La classe de l'adresse déterminée par son octet de poids fort (le plus à gauche) indique la façon dont les octets sont alloués, écrits sur 4 valeurs comme en hexadécimal pour la lisibilité mais ce sont bien des blocs de 8 octets:

- Si $0 \leqslant X < 128$: adresse de classe A

Forme	**Réseau**	Hôte	Hôte	Hôte
Binaire	**0xxxxxxx**	hôte	hôte	hôte
Décimal	**0**	hôte	hôte	hôte

  Plage d'adresse de 0.0.0.0 à 127.255.255.255

- Si $128 \leqslant X < 192$: adresse de classe B.

Réseau	**Réseau**	Hôte	Hôte
10xxxxxx	**réseau**	hôte	hôte
128	**réseau**	hôte	hôte

Plage d'adresse de 128.0.0.0 à 191.255.255.255

- Si $192 \leqslant X < 224$: adresse de classe C.

Réseau	**Réseau**	**Réseau**	Hôte
110xxxxx	**réseau**	**réseau**	hôte
192	**réseau**	**réseau**	hôte

Plage d'adresse de 192.0.0.0 à 223.255.255.255

- Si $224 \leqslant X < 240$: adresse de classe D. Cette classe d'adresse est utilisée pour le **multicast**.

Exemple: La partie en gras indique les octets réservés à l'adresse du réseau:

- **13**.102.45.177 est une adresse IP de classe A.
- **196.102.45**.13 est une adresse IP de classe C.

1.4.2 Masque de réseau

Le masque de réseau a la forme d'une adresse sur 4 octets: les bits identifiant le réseau ont pour valeur 1, et 0 sinon. Une adresse de classe C a donc pour masque par défaut : 255.255.255.0 aussi noté /24 car 8×3 octets sont à 1. Deux adresses particulières sont réservées:

1. Si tous les bits de l'ID machine sont à 1: adresse de diffusion ou broadcast. Pour s'adresser à toutes les machines.
2. Si tous les bits de l'ID machine sont à 0: adresse du réseau.

Exemple: L'adresse de classe C 192.168.10.0 laisse les 8 derniers octets pour le nom d'hôte, elle a un masque par défaut de 255.255.255.0. Les adresses 192.168.10.0 et 192.168.10.255 sont réservés respectivement comme adresse de réseau et de diffusion (ou broadcast). Cette dernier permet d'envoyer des messages à l'ensemble des machines du réseau. Il y a 256-2=254 adresses disponibles pour les machines sur ce réseau. On peut alors définir un masque pour séparer en sous-réseau.

Les masques vont permettre de définir des sous-réseaux: on pourra "déborder" sur les "octets hôtes" définis plus haut. Si on veut jusqu'à 8 sous-réseau sur ce réseau, il suffit de reprendre notre masque par défaut et de compléter avec les 3 bits de poids forts à 1, car $2^3 = 8$:

11111111	11111111	11111111	11100000
255	255	255	224
Réseau	Réseau	Réseau	sous-réseau (3bits) et hôte (5bits)

Il y aura $2^3 = 8$ sous-réseaux disponibles et $2^5 = 32$ soit 30 machines disponibles (on enlève les adresses de sous-éseau et de broadcast sur ces sous-réseaus.

Pour savoir si deux machines sont sur le même sous-réseau, on effectue un `ET` bit à bit avec le masque. Si les adresses sont les mêmes, les deux machines sont sur le même sous-réseau.

Exercices Les adresses IP 192.168.129.10, 192.168.135.200 et 192.168.145.1 dénotent-elles des machines du même sous-réseau ? Un réseau a comme masque 255.255.255.224. Combien peut-il y avoir de machines sur ce sous-réseau ? 30. On dispose d'une adresse de réseau 192.168.4.0/24 et on veut créer 3 sous-réseaux à partir de cette adresse. Quel masque doit-on utiliser ? On aura 4 sous-réseaux, il faut 2 bits pour les représenter. Le masque est 255.255.255.11000000 .

1.5 Exercice

Exercice 1 Ouvrir un shell et retrouver l'adresse IP ainsi que l'adresse MAC de la carte réseau utilisée.

Exercice 2

1. Retrouver les différents routeurs utilisés pour accéder à maths-code.fr .
2. A qui appartient le routeur auquel est connecté votre ligne ?
3. A l'aide d'un site permettant d'identifier une adresse IP comme `https://www.whois.com/whois/`, retrouver à qui appartiennent les routeurs successifs.
4. Qui est l'hébergeur de maths-code.fr ? Est-ce en France ou à l'étranger?
5. Comment une machine fait-elle le lien entre maths-code.fr et son adresse IP ?

Exercice 3 Avant de commencer l'analyse de réseau, fermez les applications réseau (navigateur, logiciels FTP, etc.)

1. Lancez Wireshark avec les droits root.
2. Sélectionner votre interface réseau, en principe `enp3s0` et ouvrir un navigateur pour vous connecter à maths-code.fr.
3. Lancez l'analyse en cliquant sur l'icône le plsu à gauche (aileron bleu). Fenêtre 1
4. Quel protocole remarquez-vous dans la fenêtre 1 ? Quelle méthode connue apparait dans la colonne 'info' ? Fenêtre 2
5. Repérez les 4 couches du modèle TCP/IP. Quelle protocole gère les ports ?
6. Cliquez sur la ligne 1 et repérez l'adresse MAC de la carte réseau de votre BOX.
7. Etes-vous en IPv6 ou IPv4?

1.6 TP FILIUS