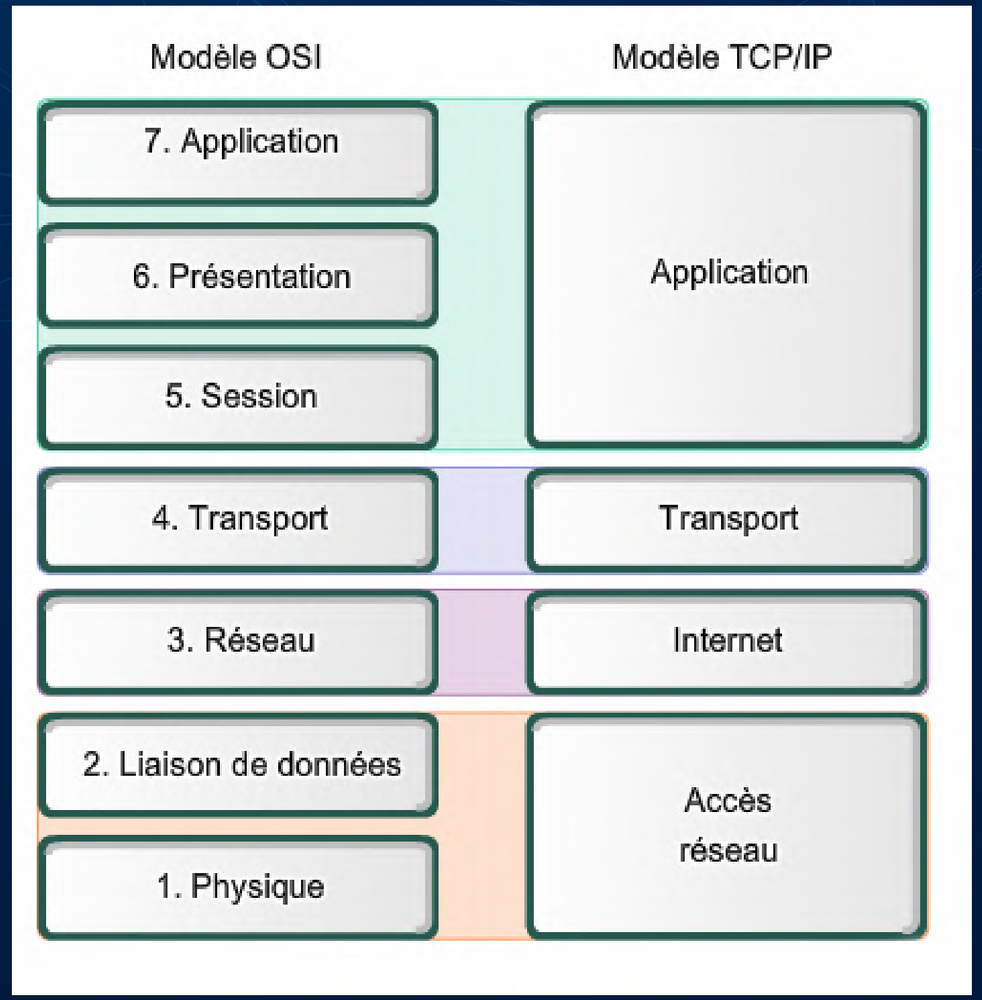
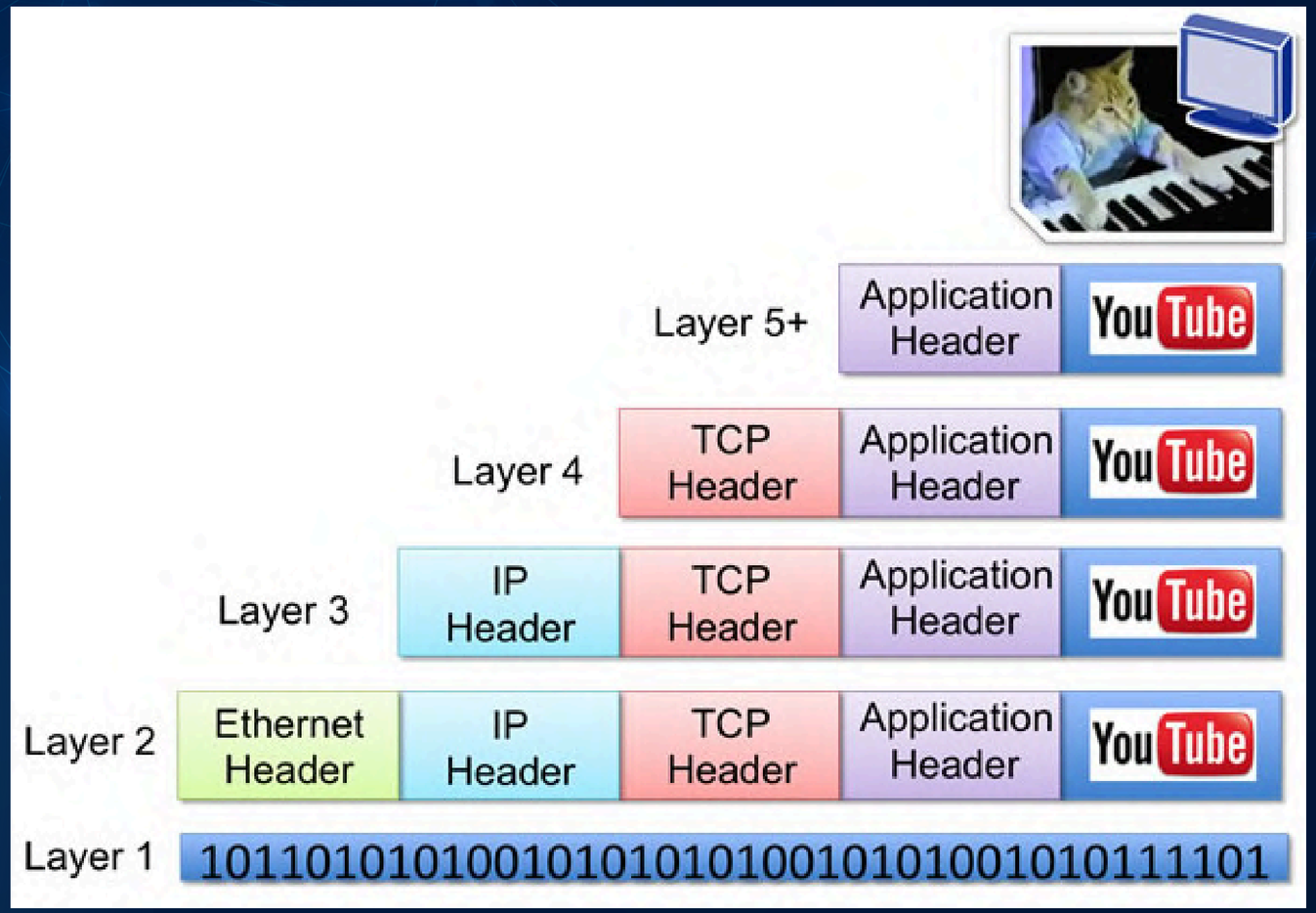
Les bases du réseau

ElPouleto & PatCarbo

Modèle OSI & TCP/IP



Encapsulation



Accès reyzo

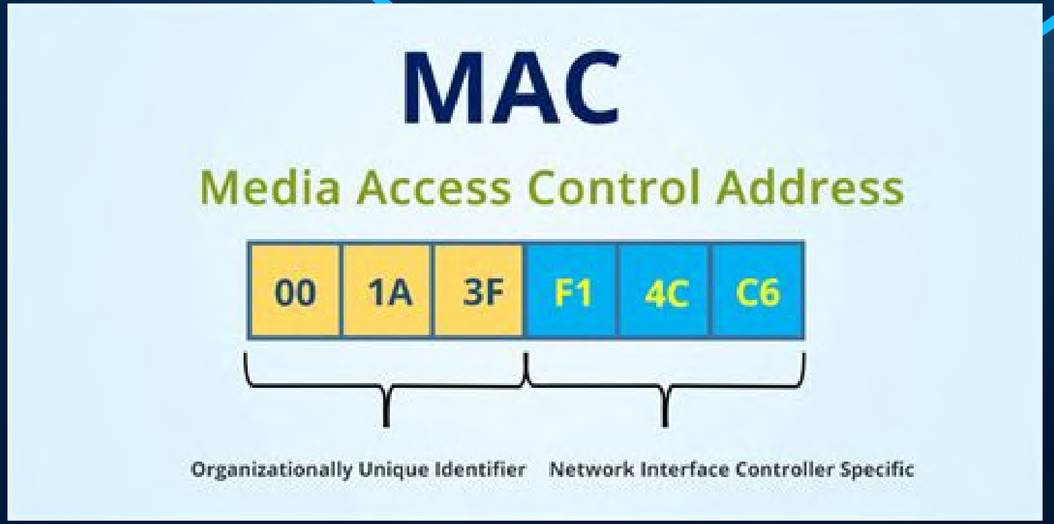
Accès reyzo

Couche physique

Comment les données sont transmises (WiFi, Câble ethernet, Fibre optique, ...)

Liaison de données

Identifie une interface dans un réseau local, définit les communication sur un réseau local



Hub VS Switch

Éclair.png

Couche 1 : Physique

Débile : il redistribue tout ce qu’il reçoit

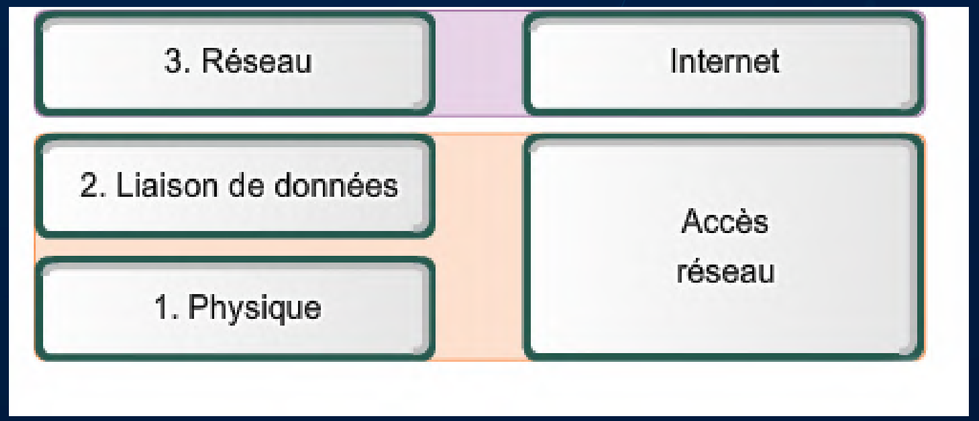
Intelligent : il envoie le paquet à la bonne interface

Couche 2 : liaison de données

Sexualité [modifier | modifier le code]

- en sexualité « être switch » signifie que dans un rapport de complémentarité la personne peut permuter les rôles (actif et/ou passif, soumis et/ou dominateur, etc.)[1].

Couche reyzo/Internet



Routeur

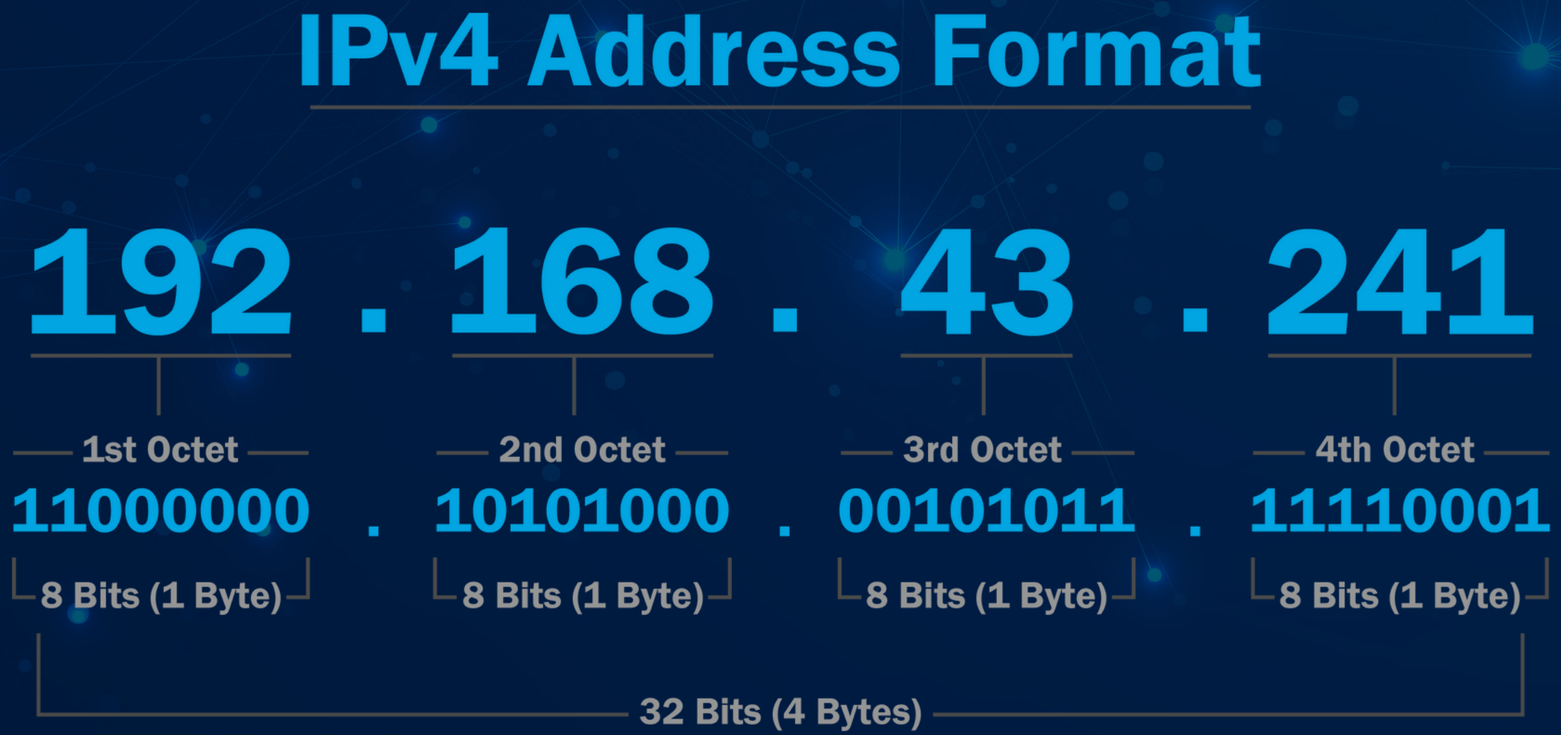
Appareil de la couche 3 (réseau)

Il relie plusieurs réseaux ou sous-réseaux

Les box internet font switch ET routeur

Adresse IP

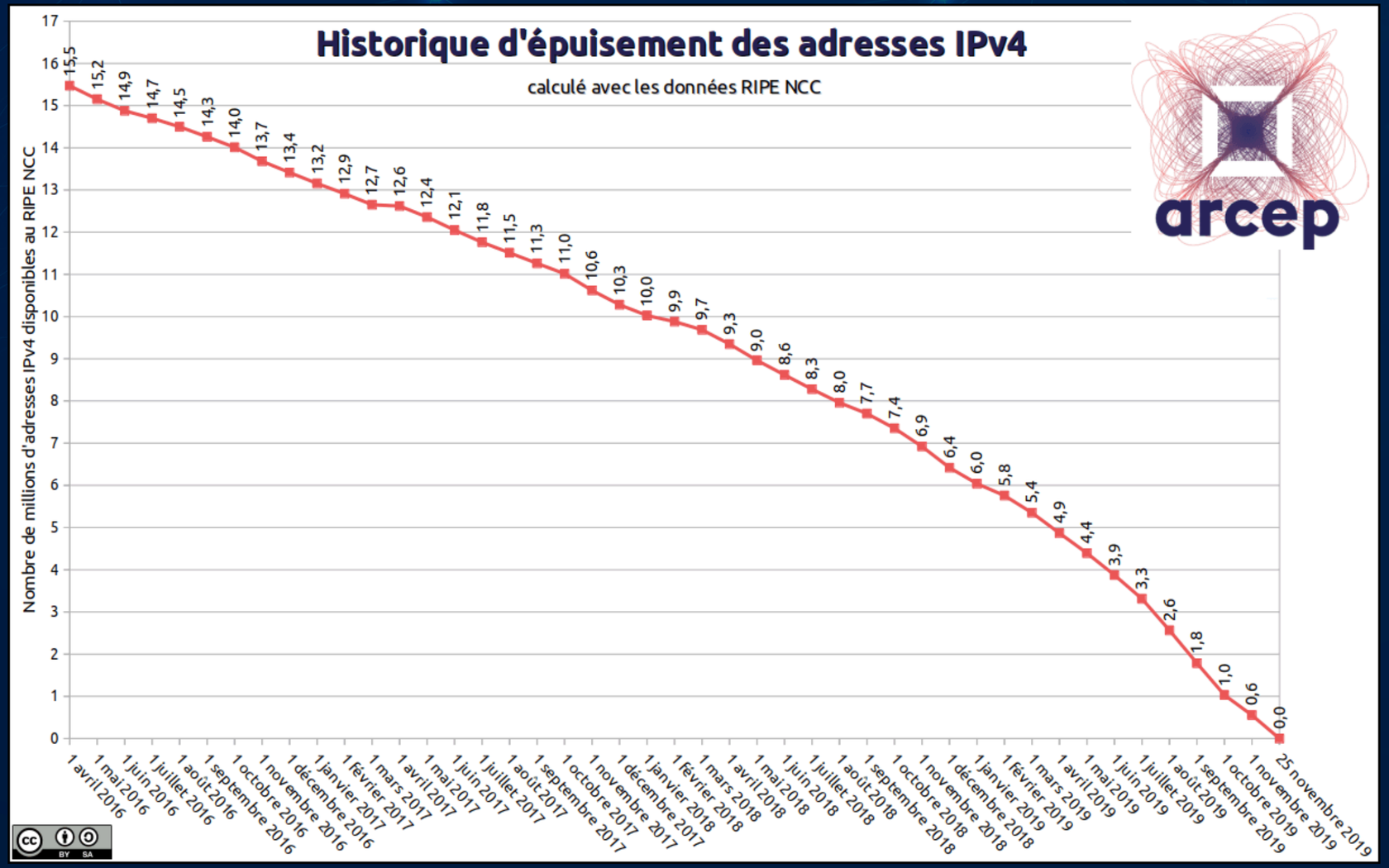
Une adresse unique par interface au sein d'un réseau



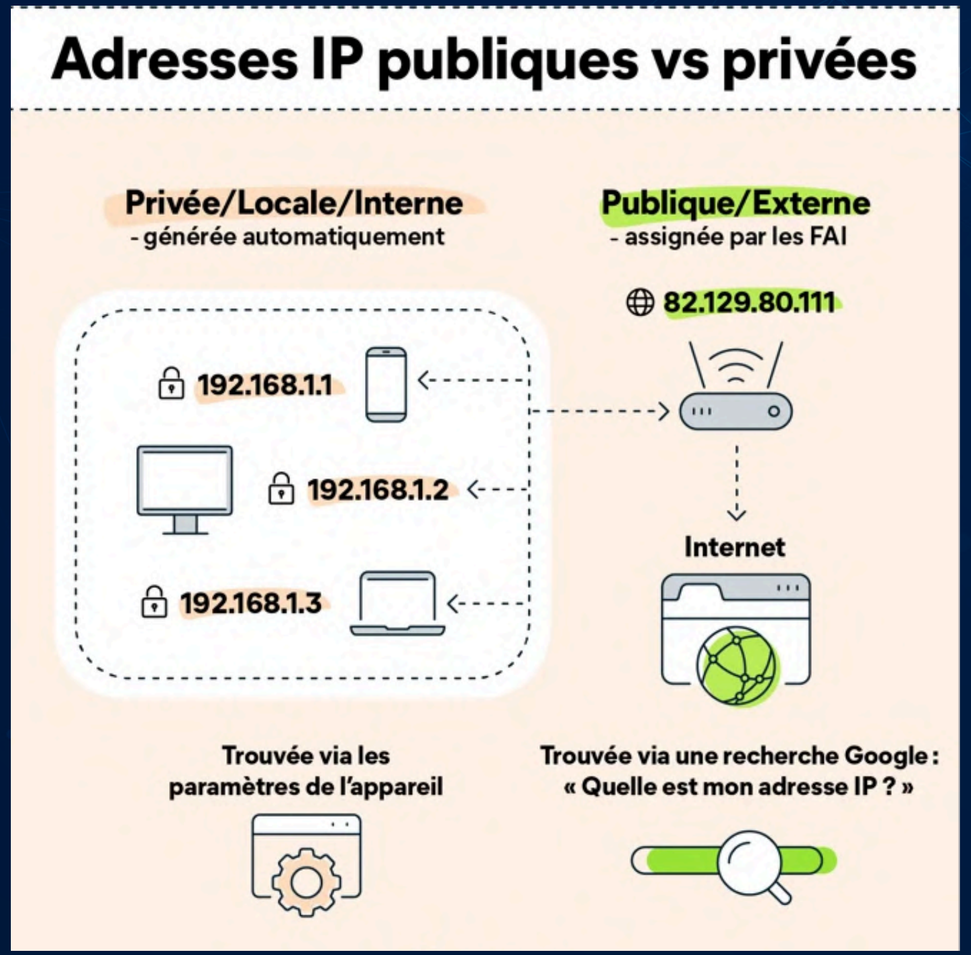
Adresse IP

2^32 possibilités ~ 4.3 milliards d'adresses possibles

Problème : ajd environ 15 milliards d'appareils connectés



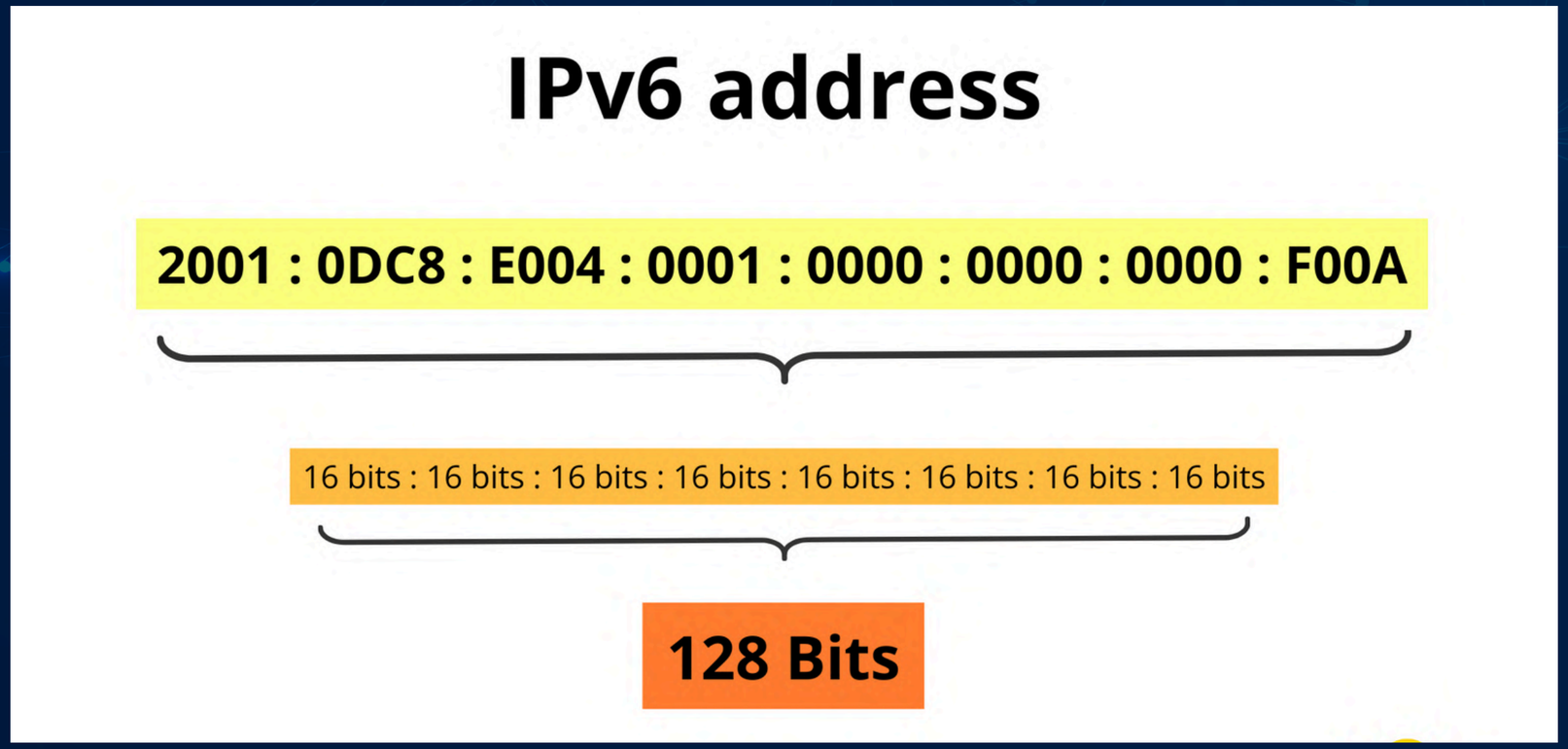
Adresse IP privée/publique



- Adresse privée : PAN, LAN -> dans un sous-réseau
  Convention : 192.168.0.0/16 ; 10.0.0.0/8 ; 172.16.0.0/12

- Relier adresses privés et publiques -> NAT (Network Address Translation)

Adresse IP



2^128 possibilités ~ bcp d'adresses possibles (3.4 * 10^38)

Masque de sous-réseau

C’est un outil utilisé pour diviser une adresse IP en deux parties : la partie réseau et la partie hôte.

Cela permet de créer des sous-réseaux au sein d’un réseau plus grand

Notation décimale	Notation binaire	Notation CIDR	Nombre de bits pour hôtes	Hôtes possibles (total – 2)
255.0.0.0	11111111.00000000.00000000.00000000	/8	24	(2^24)-2 soit 16 777 214
255.128.0.0	11111111.10000000.00000000.00000000	/9	23	8 388 606
255.192.0.0	11111111.11000000.00000000.00000000	/10	22	4 194 302
255.224.0.0	11111111.11100000.00000000.00000000	/11	21	2 097 150
255.240.0.0	11111111.11110000.00000000.00000000	/12	20	1 048 574
255.248.0.0	11111111.11111000.00000000.00000000	/13	19	524 286
255.252.0.0	11111111.11111100.00000000.00000000	/14	18	262 142
255.254.0.0	11111111.11111110.00000000.00000000	/15	17	131 070
255.255.0.0	11111111.11111111.00000000.00000000	/16	16	65 534
255.255.128.0	11111111.11111111.10000000.00000000	/17	15	32 766
255.255.192.0	11111111.11111111.11000000.00000000	/18	14	16 382
255.255.224.0	11111111.11111111.11100000.00000000	/19	13	8 190
255.255.240.0	11111111.11111111.11110000.00000000	/20	12	4 094
255.255.248.0	11111111.11111111.11111000.00000000	/21	11	2 046
255.255.252.0	11111111.11111111.11111100.00000000	/22	10	1 022
255.255.254.0	11111111.11111111.11111110.00000000	/23	09	510
255.255.255.0	11111111.11111111.11111111.00000000	/24	08	254
255.255.255.128	11111111.11111111.11111111.10000000	/25	07	126
255.255.255.192	11111111.11111111.11111111.11000000	/26	06	62
255.255.255.224	11111111.11111111.11111111.11100000	/27	05	30
255.255.255.240	11111111.11111111.11111111.11110000	/28	04	14
255.255.255.248	11111111.11111111.11111111.11111000	/29	03	6
255.255.255.252	11111111.11111111.11111111.11111100	/30	02	2

IT-CONNECT

Couche transport

4. Transport	Transport
3. Réseau	Internet
2. Liaison de données	Accès réseau
1. Physique	

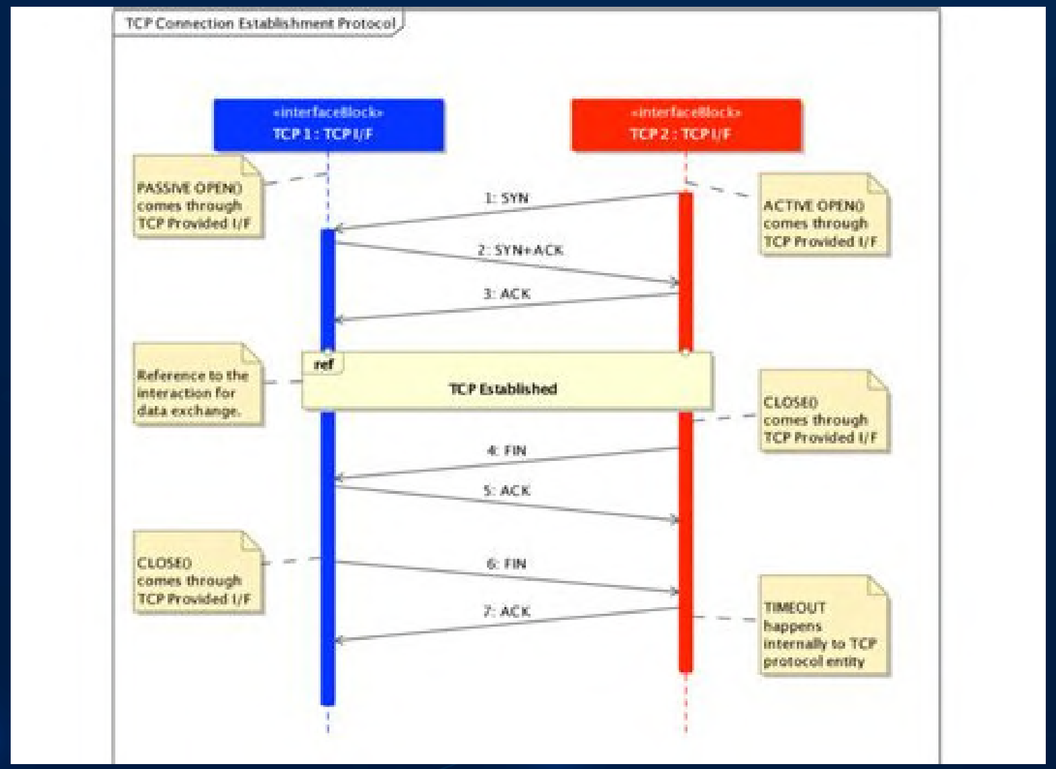
Couche transport

Protocoles chargés de la gestion des **erreurs** et du contrôle des **flux réseaux**

TCP (Transmission Control Protocol)

- FIABLE
- Contrôle des erreurs

- Lent de ouf
- Gourmand en bande passante



Couche transport

UDP (User Datagram Protocol)

- RAPIDE
- Bande passante chill

- Données peuvent ressembler à rien

NETFLIX

Couche transport

Les ports réseau

Iddentifiants numériques utilisés pour distinguer les différentes applications ou services qui communiquent sur le réseau

1. Ports 1 à 1023 : Well-Known Ports

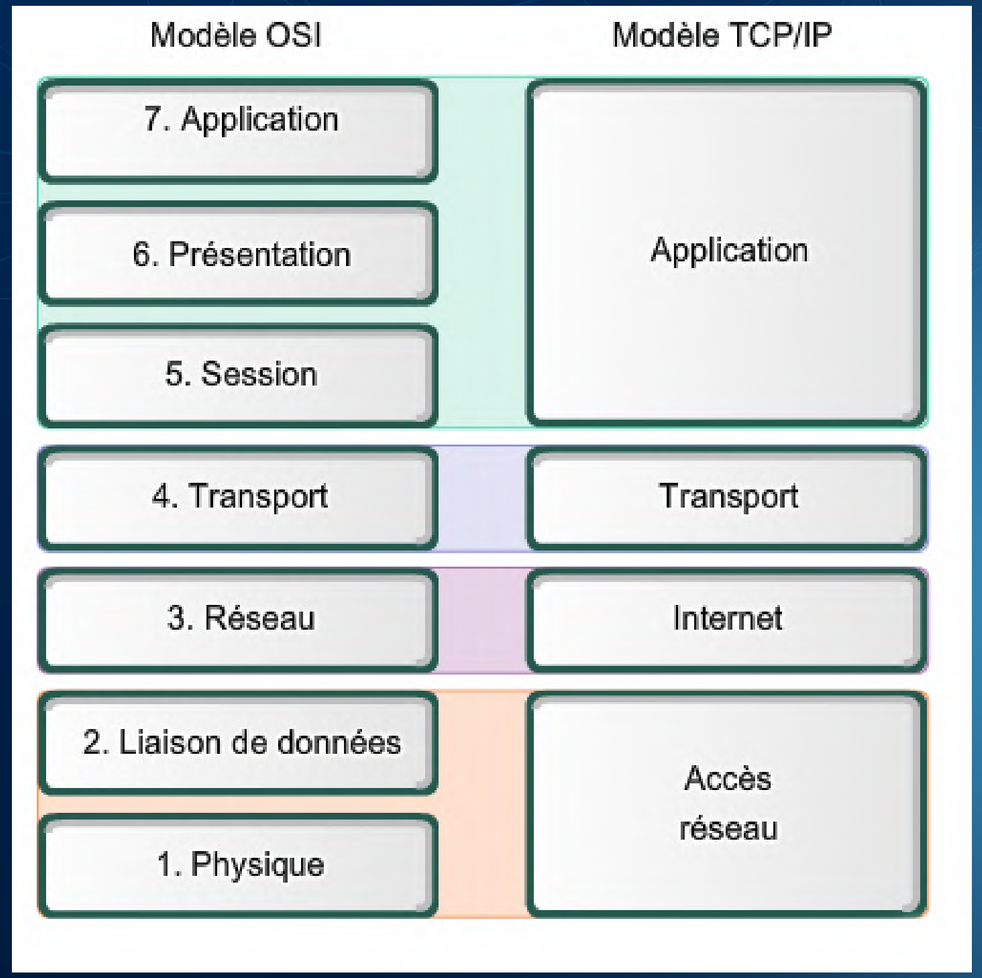
   HTTP : 80, HTTPS : 443, SSH : 22

2. Ports 1024 à 49151 : Registered Ports

   MySQL : 3306, Windows Messenger : 1026-1029

3. Ports 49152 à 65535 : Dynamic/Private Ports

Couche application



Couche Application

Interface utilisateur

Point d’accès aux services réseau pour les applications (software).

Protocoles courants

- HTTP/HTTPS : communication entre les navigateurs web et les serveurs web
- FTP : transfert de fichiers
- SMTP : transfert d’email
- DNS, DHCP .....

Fonctionnalités

Elle identifie les interlocuteurs, vérifie la disponibilité des ressources, et synchronise les communications

Kahoot

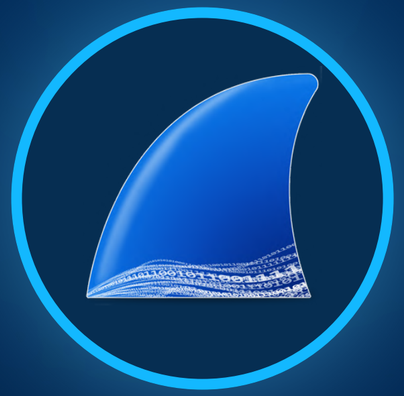
Qui a le plus gros cerveau ?

TP

Miam miam le réseau

pour les plus rapides

On teste nmap :
sudo apt install nmap (sinon sur nmap.org)
puis tester dans le terminal : nmap -v scanme.nmap.org
Puis check la doc : nmap.org/man/fr/
N’hésitez pas à poser des questions



Wireshark

- Capture de réseau
- Analyse de la capture
- Filtrer le traffic
- Décodage de certains protocoles

Installation Wireshark

Sous Ubuntu/Debian :
sudo apt install wireshark
(autres distros, regarder sur le World Wide Web)

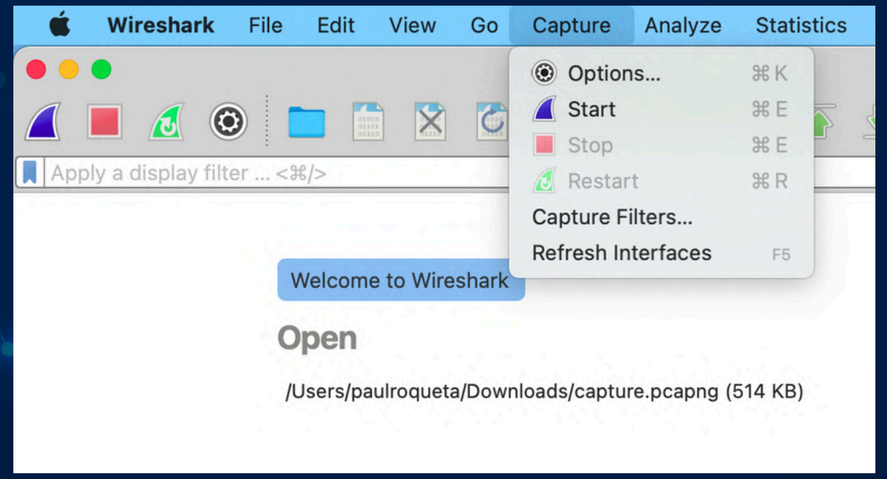
Sous Windows/macOS :
Installez la version adaptée sur https://www.wireshark.org/download.html
et exécutez le fichier exe

Place à la capture

Pour Linux, lancez wireshark (en admin)
sudo wireshark

Pour Windows, double clique sur l'icône

Capturez le réseau :
Dans la barre en haut :
Capture -> Option (CLT+K)
Puis vous sélectionnez l'interface réseau que vous voulez capturer (interface Wi-Fi par exemple)

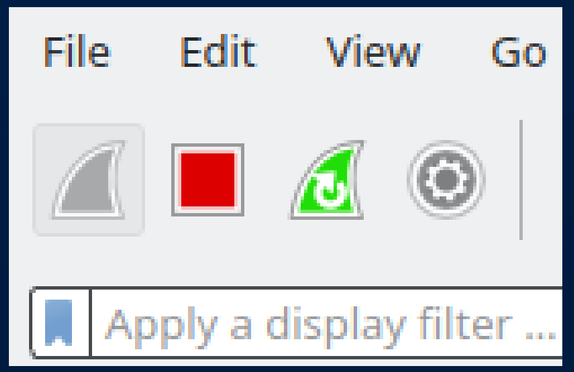


Place à la capture

Ouvrez un terminal
Ubuntu : CLT+ALT+T
Windows : Windows+R, puis tapez cmd
macOS : faîtes-vous confiance

Exécutez la commande :
ping google.com

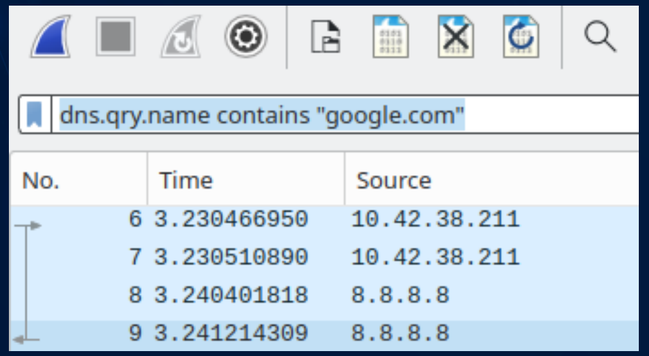
Revenez sur Wireshark et stoppez la capture. (Cliquez sur le carré rouge)
Arrêtez la commande ping, CLT+C dnas le terminal



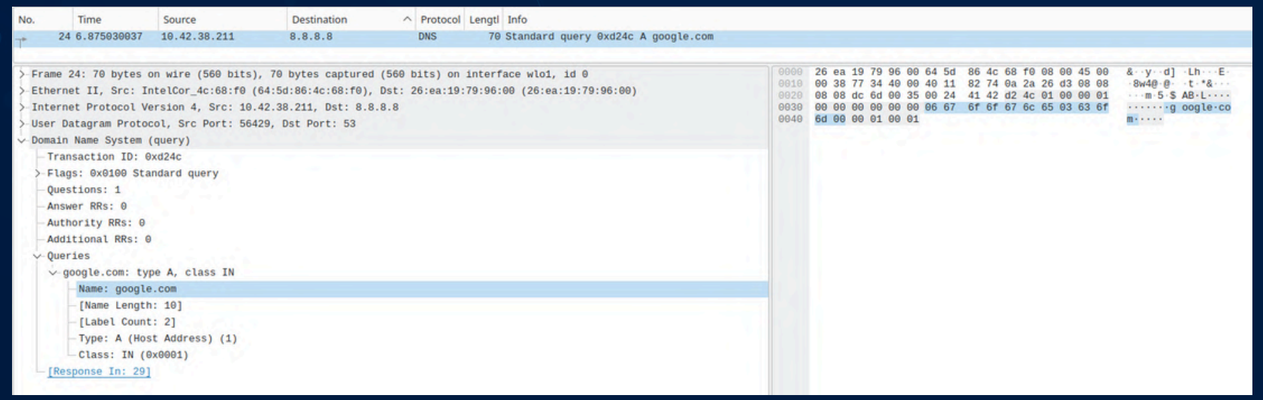
Analyse de la capture

Dans le champ filtre, copiez celui là :
dns.qry.name contains "google.com"
Appuyez sur Entrer

Que fait ce filtre ?



Cliquez sur un des paquets
Wireshark présente la donnée sous format de couche et en cliquant sur une, on peut avoir les informations des headers (ex: source, destination, taille des données, contenu ... -> les infos dépendent du protocole utilisé)



Explication

Ici nous nous intéressons au protocole DNS qui se situe à la couche application. Il sert à traduire les URL (en texte lisible par des humains) en adresse IP (qu'utilisent les machines).

Dans mon cas, 8.8.8.8 est l'adresse IPv4 publique d'un des serveurs DNS de Google.
Cette requête sert à demander : Quelle IP est associée l'URL google.com ?

NB : ici on a utilisé la commande "ping" qui utilise le protocole de couche 3, ICMP. On aurait eu le même paquet DNS si on avait taper "google.com" dans un navigateur web.

En outre, cet exemple est un prétexte pour vous montrer l'application du modèle OSI et de l'encapsulation (ici, Application : DNS; Transport: UDP; Réseau: IPv4; Accès réseau: Ethernet II)

La bisette