

Introduction au réseau

Maxime Bombar
Michaël Paulon

4 Novembre 2019



Qu'est-ce qu'un réseau ?

Définition

Un réseau informatique est un ensemble d'équipements reliés entre eux pour échanger des informations.

Protocole

Un protocole est une spécification de plusieurs règles pour un type de communication particulier. ^a

a. Wikipedia

Exemple de spécifications :

- Structure des données transmises
- Identification des participants
- Vérification ou non de l'intégrité des données transmises
- ...



Qu'est-ce qu'un réseau ?



Comment ça marche ?

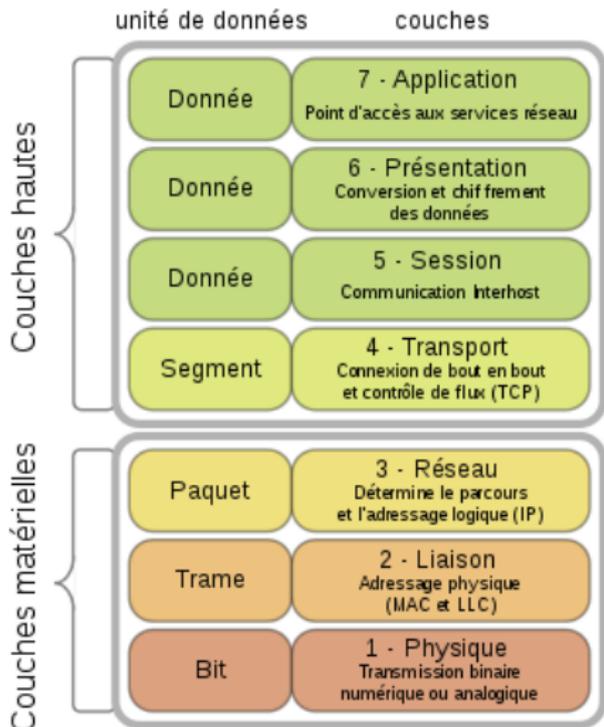
Encapsulation

Procédé consistant à inclure les données d'un protocole dans un autre protocole.^a

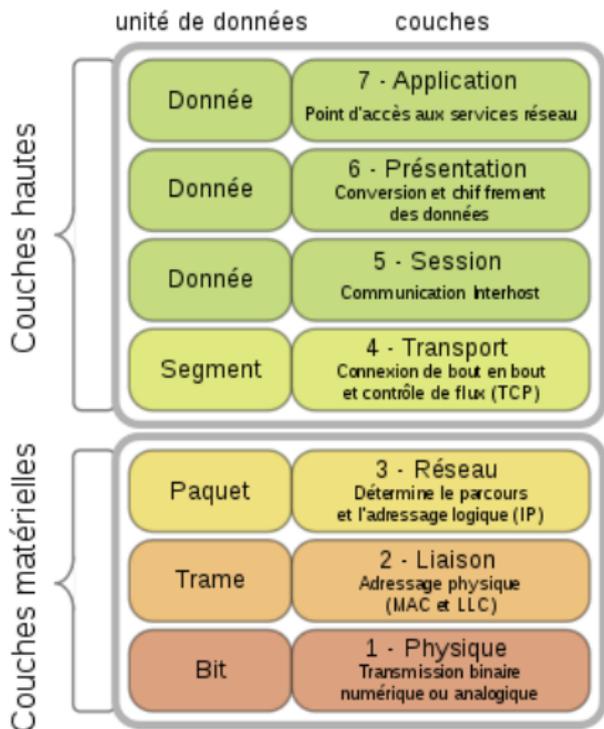
a. Wikipedia



Le modèle OSI



Le modèle OSI



Très souvent, les problèmes de réseau sont des problèmes de couche 8.



Le modèle OSI

Numéro	Couche	Identifiant	Exemples
7	Application		HTTP, FTP, DNS
6	Présentation		TLS, unicode
5	Session		RPC, SOCKS
4	Transport	Port	TCP, UDP, ICMP
3	Réseau	Adresse IP	IPv4, IPv6
2	Liaison	MAC	Ethernet
1	Physique		USB



Media Access Control

Adresse MAC

L'adresse MAC est un identifiant unique (Une pour chaque interface physique). C'est un nombre de 48 bits représenté par 6 nombres en hexadécimal.

Exemples :

- `4c:34:88:54:e8:c2` est l'adresse MAC de ma machine.
- `ff:ff:ff:ff:ff:ff` est la MAC de broadcast.



Adresse IP

IPv4

L'adresse IPv4 est un identifiant de 32 bits (4 octets). On les note par 4 nombres écrits en base 10 séparés par des points.

Exemple : 138.231.136.1 est l'adresse IPv4 de zamok.crans.org

IPv6

L'adresse IPv6 est un identifiant de 128 bits (16 octets). On les note par groupes de 2 octets écrits en hexadécimal, et séparé par des :

Exemple : 2a0c:700:0:1:1e98:ecff:fe15:2c88 est l'IPv6 de zamok.crans.org



Et vous ?

Pour UNIX

Ouvrez un terminal et tapez

```
ip a
```

Pour les windows

Ouvrez l'invite de commande (Windows + R + cmd) et tapez

```
ipconfig /all
```



Voir le réseau ?

- Une fois la machine connectée, elle voit en permanence passer des trames sur le réseau.
- Si la trame lui est destinée (bonne adresse MAC), elle le traite.
 - Si l'ip à l'intérieur est la sienne elle agit en conséquence
 - Sinon elle l'ignore ou le renvoie à la «bonne» destination (routeur)
- Sinon elle l'ignore.

Des outils pour «sniffer» le réseau

tcpdump, wireshark



Mais au fait Internet, comment ça marche ?

- Internet, c'est juste un graphe.
- Découverte des voisins avec ARP ou NDP.
- Si tout le monde était interconnecté, tout serait facile.
- Internet c'est grand.



Mais au fait Internet, comment ça marche ?

- Internet, c'est juste un graphe.
- Découverte des voisins avec ARP ou NDP.
- Si tout le monde était interconnecté, tout serait facile.
- Internet c'est grand.



Mais au fait Internet, comment ça marche ?

- Internet, c'est juste un graphe.
- Découverte des voisins avec ARP ou NDP.
- Si tout le monde était interconnecté, tout serait facile.
- Internet c'est grand.



Mais au fait Internet, comment ça marche ?

- Internet, c'est juste un graphe.
- Découverte des voisins avec ARP ou NDP.
- Si tout le monde était interconnecté, tout serait facile.
- Internet c'est grand.



Mais au fait Internet, comment ça marche ?

- Internet, c'est juste un graphe.
- Découverte des voisins avec ARP ou NDP.
- Si tout le monde était interconnecté, tout serait facile.
- Internet c'est grand.

Un petit calcul

Ipv4 = 32 bits et il en existe 2^{32} . MAC = 48 bits. On doit donc stocker un tableau de 2^{32} lignes contenant chacune 80 bits d'information. Il faudrait donc ~ 350 Gb de RAM uniquement pour stocker les voisins !



En pratique

On découpe le graphe en sous-réseaux et on stocke les voisins avec qui on communique réellement.

Faites le test !

```
arp -n
```



Sous-réseau

- Une adresse IP identifie un sous-réseau (préfixe) et la machine qui est dessus.
- Le sous-réseau est identifié par un masque : Tous les bits du préfixe sont mis à 1
 - *Exemple* : $255.255.255.0 = 2^8 = 256$ adresses
 - *Notation* : Première IP du sous-réseau + *slash* + nombre de bits du préfixe
 - *Exemple* :
 - 138.231.136.0/24
 - 2a0c:700::/32



Qu'est-ce qu'il se passe quand je branche mon câble ?

- Qu'y a-t-il au bout du câble ?
- Des switches, d'autres cables ethernet, des fibres optiques.
- Différence entre un switch et un hub ?
- Au bout de la chaîne de switches, on trouve un routeur : l'aiguilleur du sous-réseau.
- Le routeur interagit avec un pare-feu pour du filtrage fin.
- C'est aussi à ce niveau que se fait le NAT (Network Address Translation).



Qu'est-ce qu'il se passe quand je branche mon câble ?

- Qu'y a-t-il au bout du câble ?
- Des switches, d'autres cables ethernet, des fibres optiques.
- Différence entre un switch et un hub ?
- Au bout de la chaîne de switches, on trouve un routeur : l'aiguilleur du sous-réseau.
- Le routeur interagit avec un pare-feu pour du filtrage fin.
- C'est aussi à ce niveau que se fait le NAT (Network Address Translation).



Qu'est-ce qu'il se passe quand je branche mon câble ?

- Qu'y a-t-il au bout du câble ?
- Des switches, d'autres cables ethernet, des fibres optiques.
- Différence entre un switch et un hub ?
- Au bout de la chaîne de switches, on trouve un routeur : l'aiguilleur du sous-réseau.
- Le routeur interagit avec un pare-feu pour du filtrage fin.
- C'est aussi à ce niveau que se fait le NAT (Network Address Translation).



Qu'est-ce qu'il se passe quand je branche mon câble ?

- Qu'y a-t-il au bout du câble ?
- Des switches, d'autres cables ethernet, des fibres optiques.
- Différence entre un switch et un hub ?
- Au bout de la chaîne de switches, on trouve un routeur : l'aiguilleur du sous-réseau.
- Le routeur interagit avec un pare-feu pour du filtrage fin.
- C'est aussi à ce niveau que se fait le NAT (Network Address Translation).



Qu'est-ce qu'il se passe quand je branche mon câble ?

- Qu'y a-t-il au bout du câble ?
- Des switches, d'autres cables ethernet, des fibres optiques.
- Différence entre un switch et un hub ?
- Au bout de la chaîne de switches, on trouve un routeur : l'aiguilleur du sous-réseau.
- Le routeur interagit avec un pare-feu pour du filtrage fin.
- C'est aussi à ce niveau que se fait le NAT (Network Address Translation).



Qu'est-ce qu'il se passe quand je branche mon câble ?

- Qu'y a-t-il au bout du câble ?
- Des switches, d'autres cables ethernet, des fibres optiques.
- Différence entre un switch et un hub ?
- Au bout de la chaîne de switches, on trouve un routeur : l'aiguilleur du sous-réseau.
- Le routeur interagit avec un pare-feu pour du filtrage fin.
- C'est aussi à ce niveau que se fait le NAT (Network Address Translation).



Un peu de routage

- Routage *next-hop*
- En général défini par la destination
- Prise en compte de certaines options : Policy based routing et *iproute2*
- Problème s'il y a des boucles.

Table de routage

Structure de données qui associe à des préfixes IP leurs prochains voisins.

- Structure ambiguë \Rightarrow on matche le préfixe le plus spécifique (*longest-prefix-rule*).
- Route par défaut ou *default gateway*.
- 255 tables disponibles.
- Routage statique VS routage dynamique.
- Règles



Pratiquons un peu

Quelles sont mes routes ?

- *ip route show*
- *ip rule show*

Au Crans

- *gulp* le routeur principal
- *odlyd* en backup
- *ipv6-zayo*^a pour le routage IPv6.

En pratique, une passerelle gérée par *keepalived* : <Prefixe>.254

a. Ouais, faudrait qu'on change ce nom ...

Démo BGP

Table de routage de Gulp.

Et la suite ?

- Le paquet est acheminé jusqu'au destinataire à travers de nombreux routeurs.
- Celui-ci répond.

Quel chemin ai-je pris ?

tracroute <destinataire>



T'as pas pris des raccourcis là ?

- À priori vous êtes tous en wifi mais êtes pourtant bien connectés. Vous ai-je menti ?
- Si vous avez compris l'encapsulation, il suffit de changer la couche 1 (Physique) pour passer du cable au Wifi !
- Mais comment je récupère une adresse IP ?
- Plusieurs protocoles possibles, par exemple DHCP
- Quand on m'a cablé, on m'a parlé de RADIUS. C'est quoi ?
- Un protocole qui gère les autorisations et authentications des utilisateurs sur un réseau. Il mérite un séminaire à part entière !



T'as pas pris des raccourcis là ?

- À priori vous êtes tous en wifi mais êtes pourtant bien connectés. Vous ai-je menti ?
- Si vous avez compris l'encapsulation, il suffit de changer la couche 1 (Physique) pour passer du cable au Wifi !
- Mais comment je récupère une adresse IP ?
- Plusieurs protocoles possibles, par exemple DHCP
- Quand on m'a cablé, on m'a parlé de RADIUS. C'est quoi ?
- Un protocole qui gère les autorisations et authentications des utilisateurs sur un réseau. Il mérite un séminaire à part entière !



T'as pas pris des raccourcis là ?

- À priori vous êtes tous en wifi mais êtes pourtant bien connectés. Vous ai-je menti ?
- Si vous avez compris l'encapsulation, il suffit de changer la couche 1 (Physique) pour passer du cable au Wifi !
- Mais comment je récupère une adresse IP ?
- Plusieurs protocoles possibles, par exemple DHCP
- Quand on m'a cablé, on m'a parlé de RADIUS. C'est quoi ?
- Un protocole qui gère les autorisations et authentications des utilisateurs sur un réseau. Il mérite un séminaire à part entière !



T'as pas pris des raccourcis là ?

- À priori vous êtes tous en wifi mais êtes pourtant bien connectés. Vous ai-je menti ?
- Si vous avez compris l'encapsulation, il suffit de changer la couche 1 (Physique) pour passer du cable au Wifi !
- Mais comment je récupère une adresse IP ?
- Plusieurs protocoles possibles, par exemple DHCP
- Quand on m'a cablé, on m'a parlé de RADIUS. C'est quoi ?
- Un protocole qui gère les autorisations et authentications des utilisateurs sur un réseau. Il mérite un séminaire à part entière !



T'as pas pris des raccourcis là ?

- À priori vous êtes tous en wifi mais êtes pourtant bien connectés. Vous ai-je menti ?
- Si vous avez compris l'encapsulation, il suffit de changer la couche 1 (Physique) pour passer du cable au Wifi !
- Mais comment je récupère une adresse IP ?
- Plusieurs protocoles possibles, par exemple DHCP
- Quand on m'a cablé, on m'a parlé de RADIUS. C'est quoi ?
- Un protocole qui gère les autorisations et authentications des utilisateurs sur un réseau. Il mérite un séminaire à part entière !



T'as pas pris des raccourcis là ?

- À priori vous êtes tous en wifi mais êtes pourtant bien connectés. Vous ai-je menti ?
- Si vous avez compris l'encapsulation, il suffit de changer la couche 1 (Physique) pour passer du cable au Wifi !
- Mais comment je récupère une adresse IP ?
- Plusieurs protocoles possibles, par exemple DHCP
- Quand on m'a cablé, on m'a parlé de RADIUS. C'est quoi ?
- Un protocole qui gère les autorisations et authentications des utilisateurs sur un réseau. Il mérite un séminaire à part entière !



Ports ¹

- Avec uniquement IP, on n'a aucune information sur le programme utilisé.
- Couche 4 : Charnière entre la partie réseau, et la partie applicative.
- On utilise des ports (identifiés par un numéro de 16 bits) pour identifier les « points d'écoute »
- En dessous de 1024, les ports sont réservés (liste dans `/etc/services/`).

Quelles applications écoutent et sur quels ports ?

netstat



1. Vous commencez à m'ennuyez avec le port

User Datagram Protocol

Envoie les données d'un couple (IP, Port) vers un autre couple (IP, port).

Encapsulé dans un paquet IP.

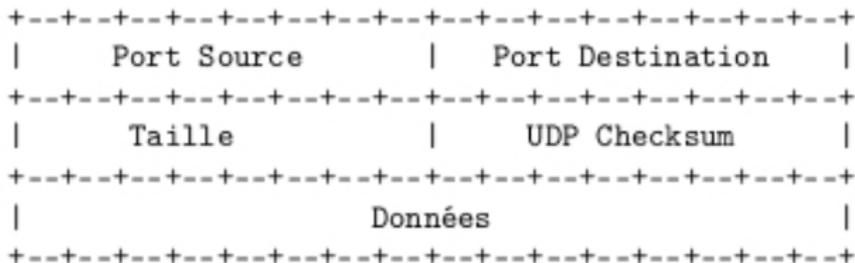


FIGURE – Structure d'un datagramme UDP



User Datagram Protocol

- **Avantage** : rapidité
- **Inconvénient** : Ne garantit pas l'ordre ni l'exactitude des données reçues.
- **Utilisation** :
 - Streaming
 - Jeux en ligne
 - DNS
 - ...



UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- You might not get it....



UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- You might not get it....



UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- You might not get it....



UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- To get to the other side. »
- ...
- « Why did the chicken cross the road ?



UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- To get to the other side. »
- ...
- « Why did the chicken cross the road ?



UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- To get to the other side. »
- ...
- « Why did the chicken cross the road ?



UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- To get to the other side. »
- ...
- « Why did the chicken cross the road ?



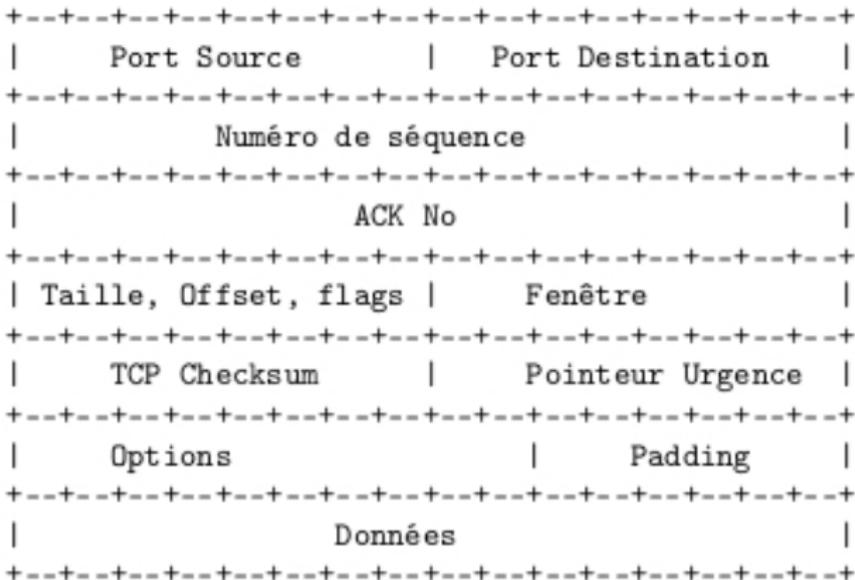
UDP joke

- Hi, would you like to hear a UDP joke ?
- Yes, I would like to hear a UDP joke.
- To get to the other side. »
- ...
- « Why did the chicken cross the road ?



Transmission Control Protocol

- Chaque paquet est vérifié
- L'ordre est contrôlé
- Début et fin de la connexion sont clairement définis.
- On définit une quantité maximale de données à envoyer.



TCP Handshake

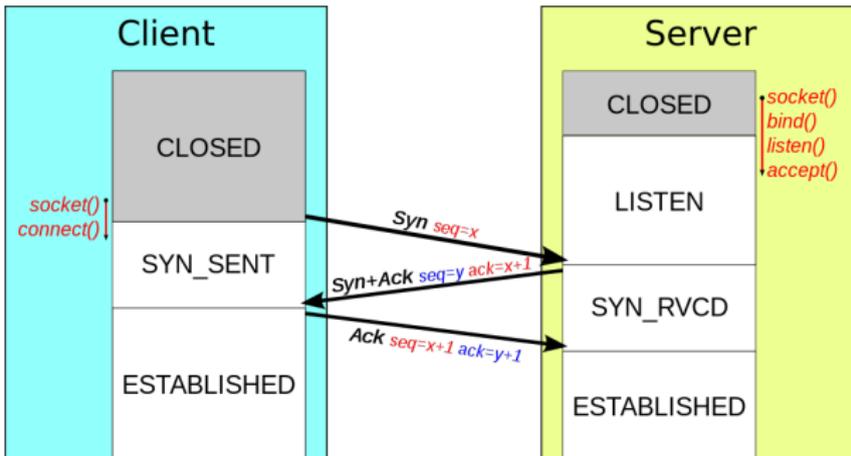


FIGURE – Établissement d'une connexion TCP



TCP Handshake

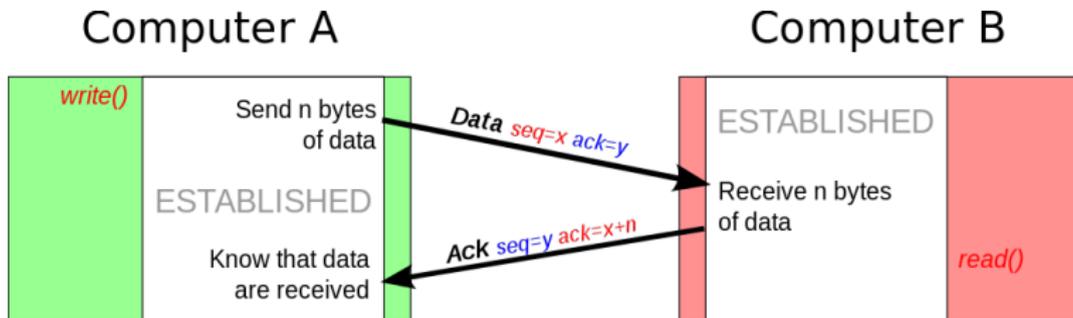


FIGURE – Transfert des données



TCP Handshake

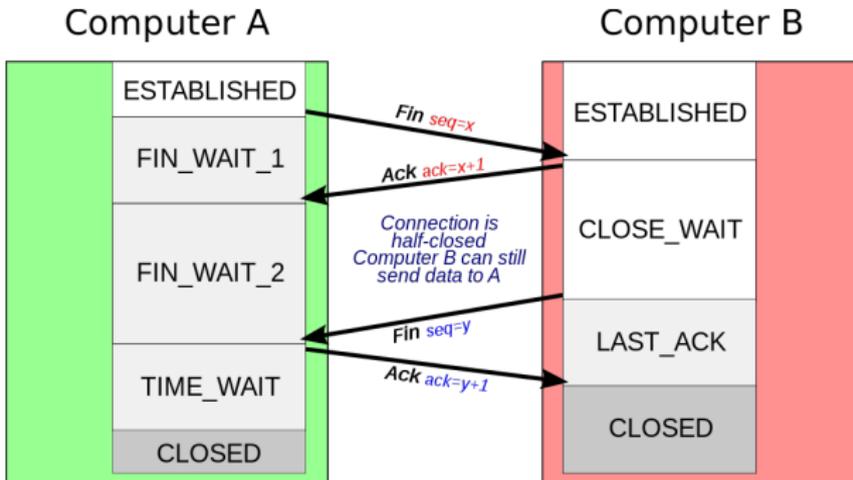


FIGURE – Cloture d'une connexion TCP



TCP joke

- Hi, I'd like to hear a TCP joke.
- Hello, would you like to hear a TCP joke ?
- Yes, I'd like to hear a TCP joke.
- Ok, I will tell you a TCP joke.
- Ok, I will hear a TCP joke.
- Are you ready to hear a TCP joke ?
- Yes, I am ready to hear a TCP joke.
- Ok, I am about to send the TCP joke. It will last 10 seconds and ends with a punchline.
- Ok, I am ready to get your 10 second-long TCP joke ending with a punchline.
- I'm sorry, your connection has timed out ...
- ... Hello, would you like to hear a TCP joke ?



Un tunnel ? des ports ? Et quoi après, des ponts ?

Un tunnel est une encapsulation de données d'un protocole dans un autre de même couche, ou de couche supérieur.

Pourquoi faire ?

- Faire transiter un protocole par un réseau qui ne le supporte pas.
- Passer un parefeu.
- Chiffrer des données.

Exemples :

- Protocole 6in4 pour faire de l'IPv6 quand le monde autour ne le supporte pas (Hurricane Electric).
- VPN : Au Crans on utilise un VPN avec wireguard pour intégrer *Sputnik* (OVH) au réseau local adm.
- Proxy SOCKS



Un exemple important : Proxy SOCKS

The screenshot shows the 'Connection Settings' dialog box with the 'Manual proxy configuration' option selected. The 'SOCKS Host' is set to 'localhost' and the 'Port' is '1080'. The 'SOCKS v5' radio button is selected. There are also fields for HTTP, SSL, and FTP proxies, all currently set to 'Port 0'. At the bottom, there are 'Help', 'Cancel', and 'OK' buttons.

- `ssh -D <port> login@host`
- Permet par exemple d'accéder à des applications campus-only !
- Ou encore d'accéder à des sites web uniquement sur le VLAN adm (backuppc, imprimante etc ...)



S'amuser à tester des trucs

Un outil magique en Python

```
sudo apt install python3-scapy  
sudo scapy3 (Ou dans un script python)
```

Scapy permet de forger, envoyer et de disséquer des paquets, et fournit un joli export en pdf !



Merci de votre attention !

