Ports 0-1023 généralement réservés par l’OS.

1024-49151 : Users & users process

1024 – 5000 : ports dits « éphémères »

Open pots should remain silent when receiveing a lone FIN packet (RFC 793)

RST ACK sent from closed ports.Open ports remain silent

Appliance : solution hard + soft

A mettre dans processus du kernel ou de linux working :

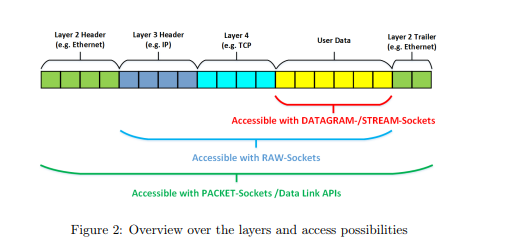
Tous les processus d’un cgroupe ne peuvent le quiter (root). Enfant hérite du cgroup de ses parents.

Car un processus peut se renommer, peut devenir enfant d’INIt, donc l’affiliation devient difficile.

Systemd-cgls : affichage des cgroups

**Network**

Enp0s1 : ethernet bus 0 slot 1



Kernel doit être compilé pour accepter l’utilisation des sockets RAW.

UNIX\_SOCKET : mode utilisateur

RAW\_SOCKET : couche 3

PACKET\_SOCKET : couche 2

Librairies : Libpcap, libnet.

IRQ ok quand peu de traffic, polling sinon avec buffer conséquent. (NAPI active polling au dela d’un certain seuil)

NIC envoie un signal à la réception d’un paquet.

* 1 ksoftIRQd s’occupe de tourner en boucle sur chaque CPU : permet de soulager l’interrupt handler qui va bloquer les autres IRQ.KsoftIRQ s execute à un haut niveau de PRIO mais pas autant que le handler d’IRQ, et il tourne avec IRQ activés.
* 1 structure softnet\_data crée sur chaque CPU (qui contient entre autre un poll\_list).

Linux utilise NAPI :permet d’éviter les tempêtes IRQ ( linux utilise les IRQ et au dela d’un certain seuil utilise NAPI : sondage du device ethernet toutes les X secondes : permet en gros de traiter plusieurs paquets d’un coup plutôt que un par un : technique du polling : mais attention si le buffer est trop plein : pertes de paquets !)