Introduction au réseau

Maxime Bombar

13 Janvier 2021

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 de l'intégrité des données transmises
- ...

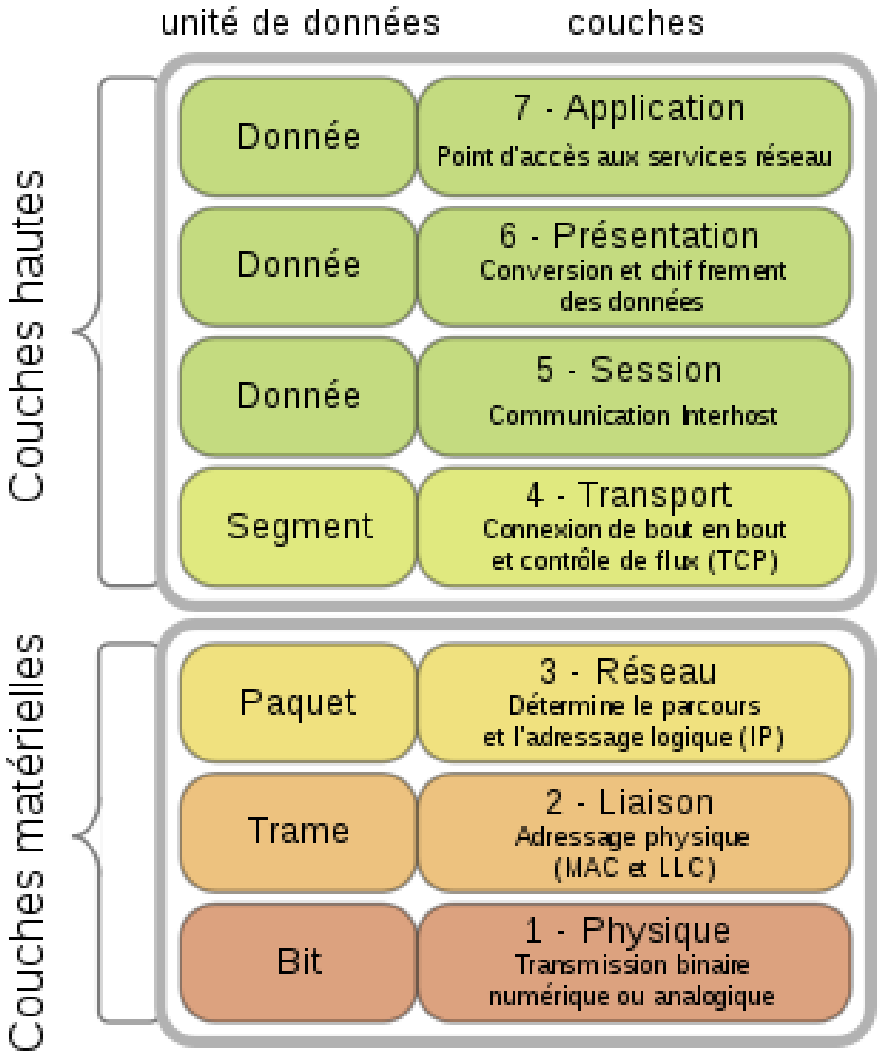
Comment ça marche ?

Encapsulation

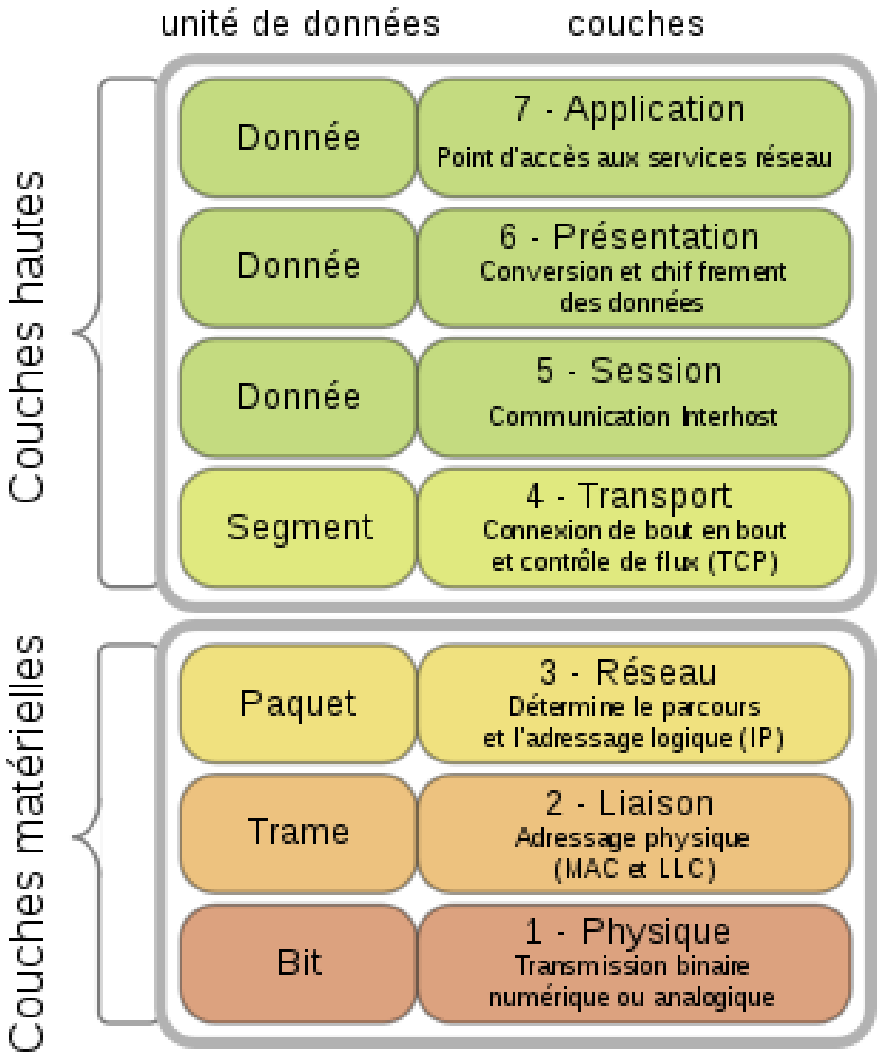
Procédé consistant à inclure les données d'un protocole dans un autre protocole. [a]

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	Addresse IP	IPv4, IPv6
2	Liaison	MAC	Ethernet
1	Physique		USB

Media Access Control

Adresse MAC

L'addresse 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'addresse MAC de ma machine.
- `ff:ff:ff:ff:ff:ff` est la MAC de broadcast.

Addresse IP

IPv4

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

Exemple : `185.230.79.1` est l'addresse IPv4 de zamok.crans.org

IPv6

L'addresse 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:700:2:0:ec4:7aff:fe59:a1ad` 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 destiné (bonne addresse MAC), elle le traite.
  - Si l'ip à l'interieur 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.

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 $\sim$ 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 (Dans le paquet *net-tools* sous Debian)

Sous-réseau

- Une addresse IP identifie un sous-réseau (préfixe) et la machine qui est dessus.
- Le sous-réseau est identifié par un masque : Tous les bits du prefixe sont mis à 1
  - *Exemple :* 255.255.255.0 $= 2^8 =$ 256 addresses
  - *Notation :* Première IP du sous-réseau + *slash* + nombre de bits du préfixe
  - *Exemple :*
    - `185.230.79.0/24`
    - `2a0c:700::/32`

Il se passe quoi quand je branche mon cable ?

Router, un défi pour la couche 3

- **Rappel :** Internet, c'est un gros graphe.
- **Objectif :** (Plus court) chemin entre deux points.
- Il faut éviter les boucles.

Router, un défi pour la couche 3

- **Rappel :** Internet, c'est un gros graphe.
- **Objectif :** (Plus court) chemin entre deux points.
- Il faut éviter les boucles.

Problèmes :

- Très gros : On ne stocke pas tout le monde –> Systèmes Autonomes (AS).
- Pas assez d'IPs pour tout le monde –> Ip privées.

Un peu de routage

On stocke les routes dans une **table de routage**

- Routage défini par la **destinatination** :
  « Je suis à Paris, je veux aller Massy –> Prendre le RER B »
- Routage par **défaut** :
  « Je suis à Paris, je veux aller à Saclay –> Dans le doute, prendre le RER B jusqu'à Massy »
- Plus compliqué ? **Policy-based routing.** :
  « Pour aller à Massy, prendre le RER B, sauf si on vient d'Austerlitz, auquel cas prendre le RER C. »

Un peu de routage

On stocke les routes dans une **table de routage**

- Routage défini par la **destinatination** :
  « Je suis à Paris, je veux aller Massy –> Prendre le RER B »
- Routage par **défaut** :
  « Je suis à Paris, je veux aller à Saclay –> Dans le doute, prendre le RER B jusqu'à Massy »
- Plus compliqué ? **Policy-based routing.** :
  « Pour aller à Massy, prendre le RER B, sauf si on vient d'Austerlitz, auquel cas prendre le RER C. »

Un peu de routage

On stocke les routes dans une **table de routage**

- Routage défini par la **destinatination** :
  « Je suis à Paris, je veux aller Massy –> Prendre le RER B »
- Routage par **défaut** :
  « Je suis à Paris, je veux aller à Saclay –> Dans le doute, prendre le RER B jusqu'à Massy »
- Plus compliqué ? **Policy-based routing.** :
  « Pour aller à Massy, prendre le RER B, sauf si on vient d'Austerlitz, auquel cas prendre le RER C. »

Le routeur, l'aiguilleur de la couche 3

- Routage externe : Routage entre AS.
- Routage interne : Routage au sein d'un AS.
- Les AS s'échangent leurs routes : BGP.

- *Crans : Passez par moi pour contacter 185.230.76.0/22.*
- *Zayo : ok j'ai compris, je dirais ça à ceux qui me contacteront. En attendant voici les routes pour internet.*

Pratiquons un peu

Quelles sont mes routes ?

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

Au Crans

Trois routeurs pour de la redondance. On utilise le logiciel Bird pour faire du BGP avec Zayo.

Pratiquons un peu

Quelles sont mes routes ?

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

Au Crans

Trois routeurs pour de la redondance. On utilise le logiciel Bird pour faire du BGP avec Zayo.

DEMO table routeur-sam

Et la suite ?

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

Quel chemin ai-je pris ?

traceroute <destinataire>

T’as pas pris des raccourcis là ?

- Mais c’est bizarre ce que tu dis, tu parles de cable. Comment ça marche en wifi ?
- 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

T'as pas pris des raccourcis là ?

- Mais c'est bizarre ce que tu dis, tu parles de cable. Comment ça marche en wifi ?
- 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

T'as pas pris des raccourcis là ?

- Mais c'est bizarre ce que tu dis, tu parles de cable. Comment ça marche en wifi ?
- 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

T’as pas pris des raccourcis là ?

- Mais c’est bizarre ce que tu dis, tu parles de cable. Comment ça marche en wifi ?
- 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

TCP-UDP et la couche 4

- Un identifiant : Le port.
- Un outil : *netstat -lapute*

- 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 identifiers les « points d'écoute »
- En dessous de 1024, les ports sont réservés (liste dans `/etc/services/`).

User Datagram Protocol

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

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.

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.

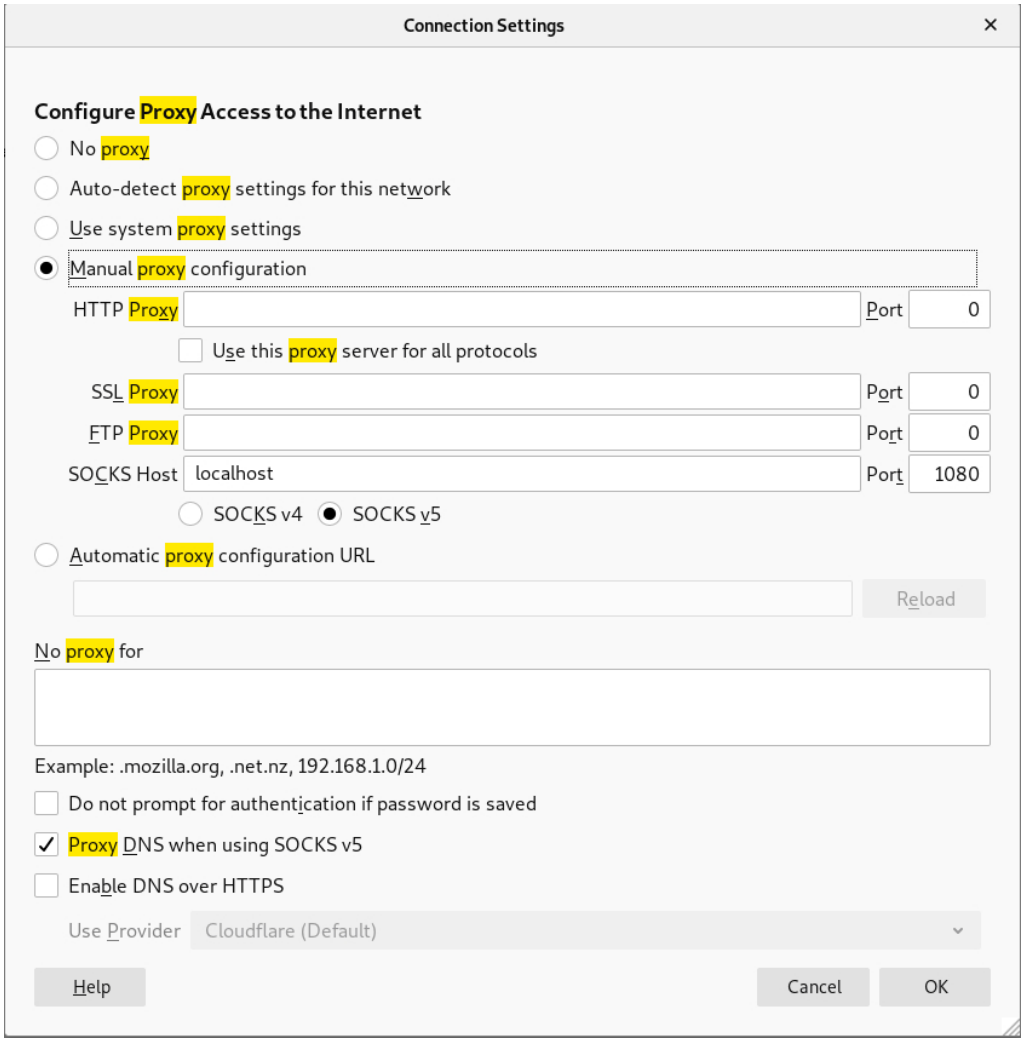
Pourquoi faire ?

- 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, wireguard pour intégrer *Sputnik* (OVH) au réseau local adm.
- Proxy SOCKS

Un exemple important : Proxy SOCKS



- *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 !