

A yellow L-shaped line consisting of a vertical segment on the left and a horizontal segment on top, positioned in the upper-left area of the slide.

# Formation TCP/IP

---

Eloïse & Martin  
9 novembre 2021

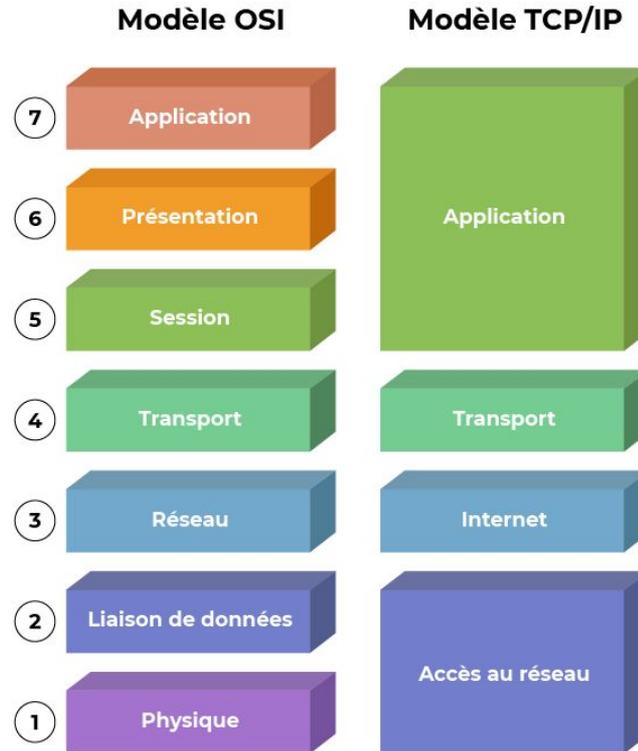
A yellow L-shaped line consisting of a vertical segment on the right and a horizontal segment on the bottom, positioned in the lower-right area of the slide.

# Sommaire

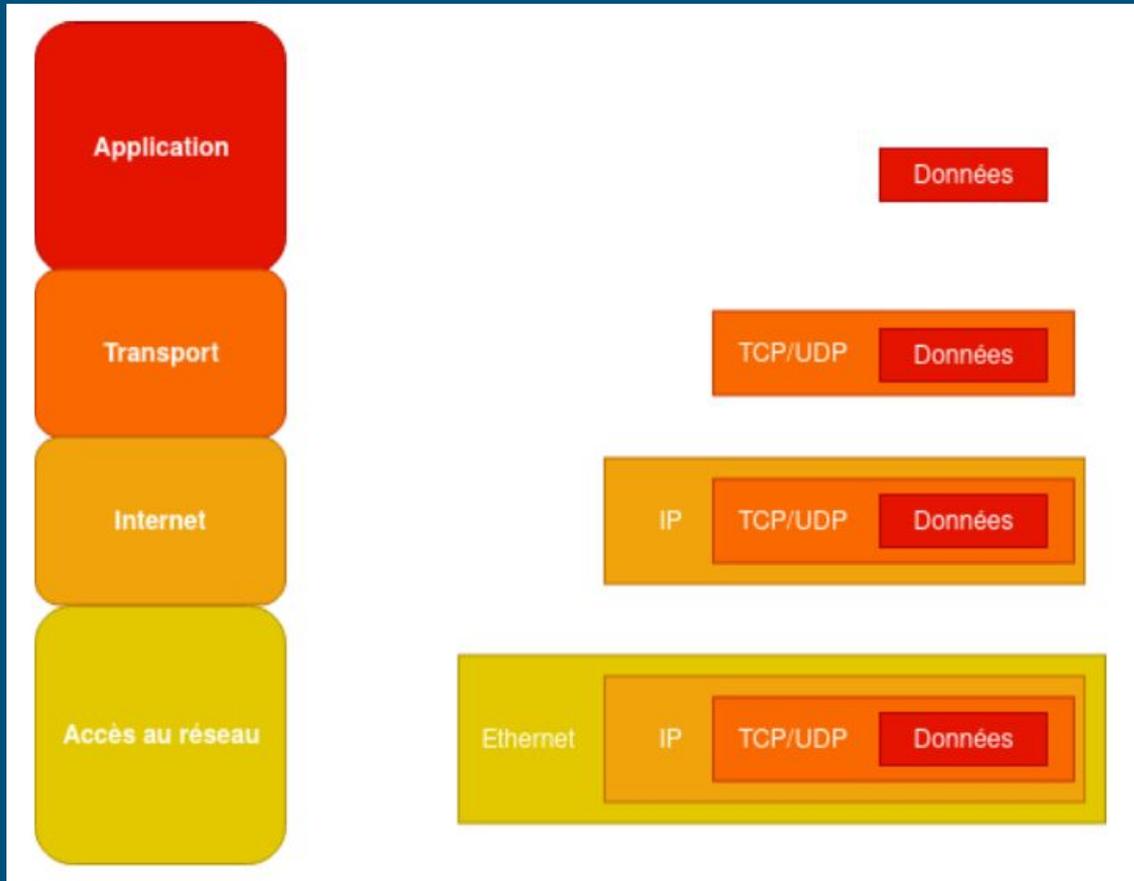
---

- Modèle en couches
- Couche 1 - Accès au réseau
- Couche 2 - Internet
- Couche 3 - Transport de données
- Couche 4 - Application

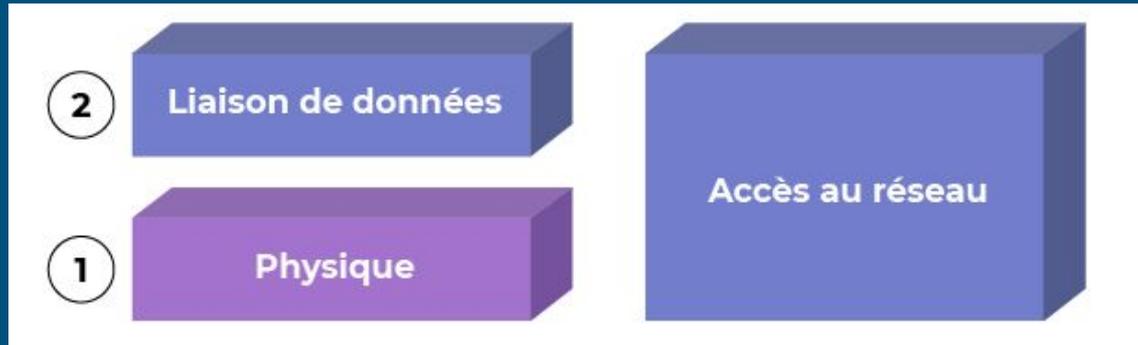
# Modèle OSI et modèle TCP/IP



# L'encapsulation



# La couche accès au réseau

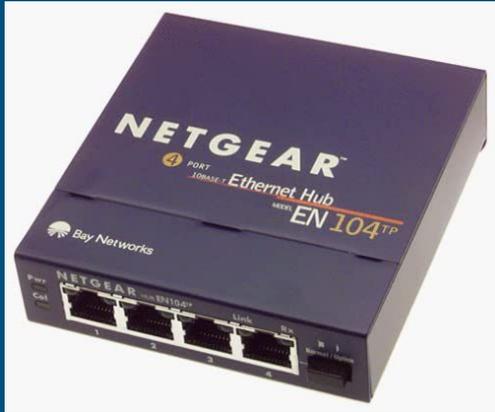


**Couche physique** : achemine signaux électriques

**Couche liaison de données** : communication entre équipements de même sous-réseau

# Comment on communique ?

- **Identification** : adresse MAC (ex : 8C-8C-AA-E6-D9-CE)  
Adresse MAC de broadcast : FF-FF-FF-FF-FF-FF
- **Equipements** :



**Le hub**

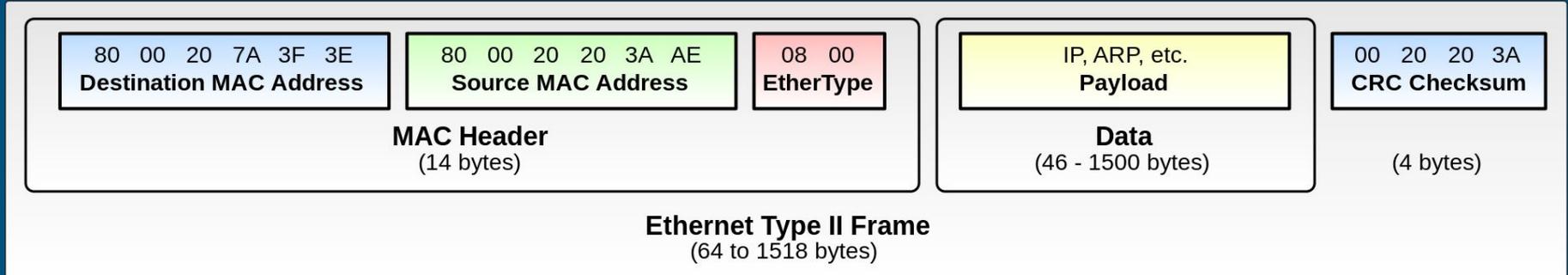
Redistribue l'information à tout le monde



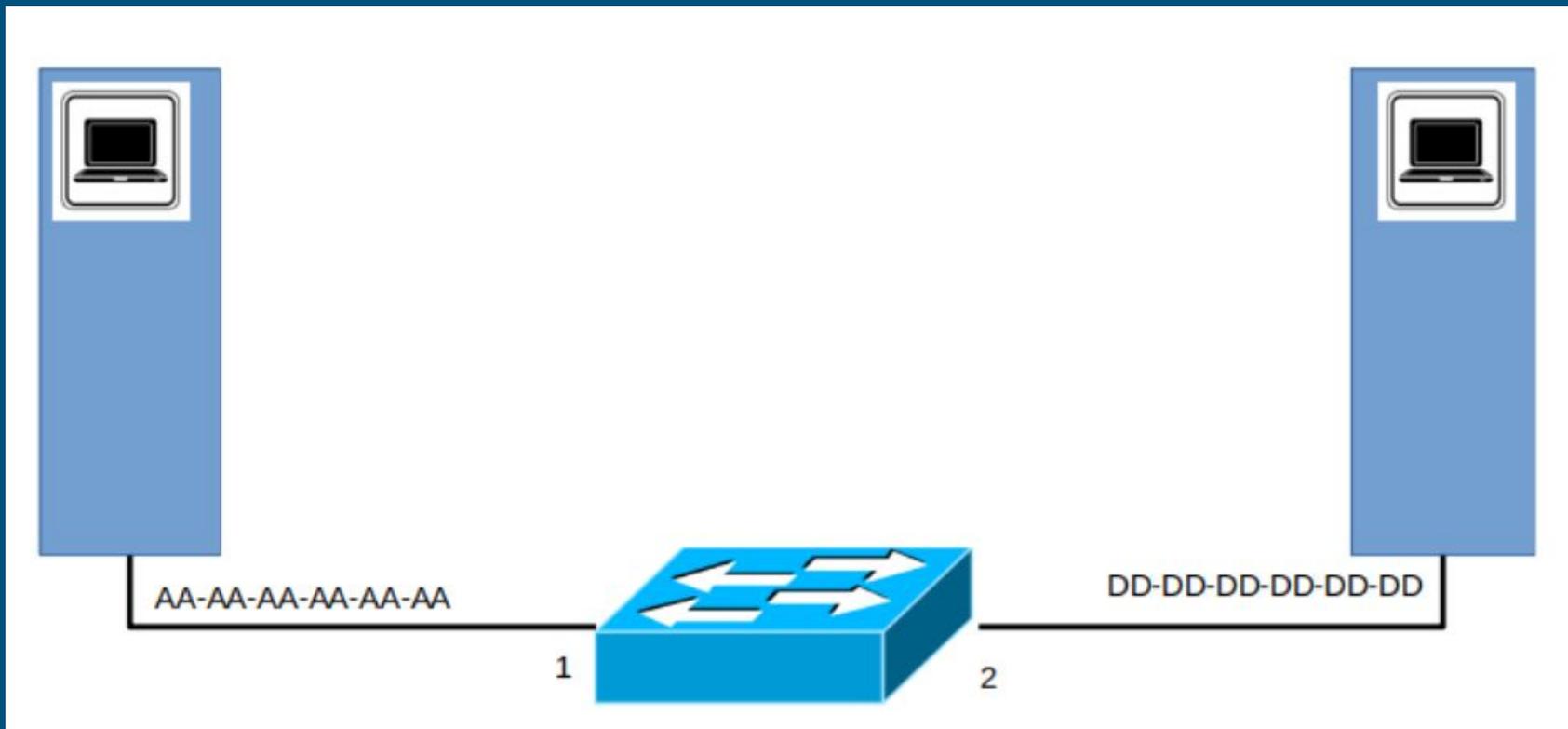
**Le switch**

Redirige l'information grâce à sa table de commutation

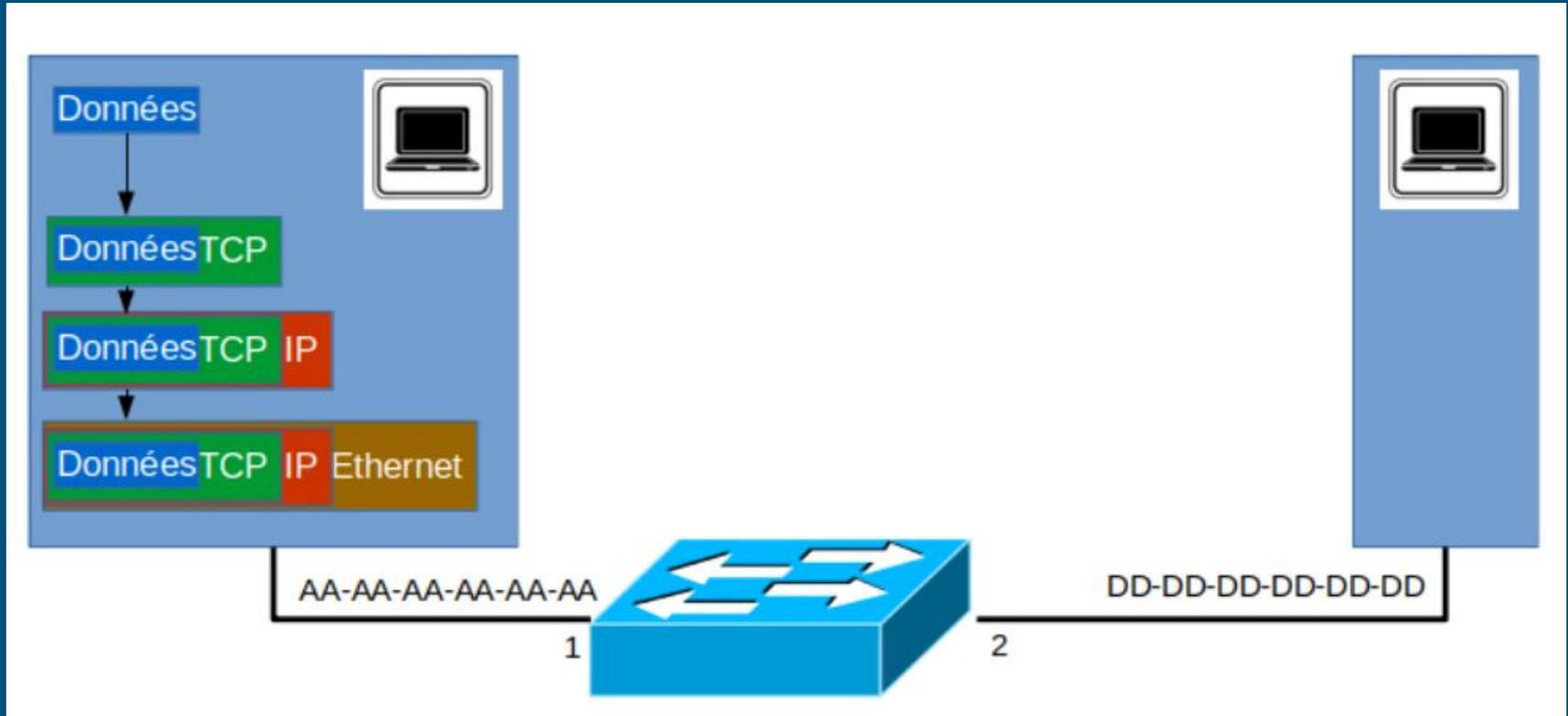
# L'entête Ethernet



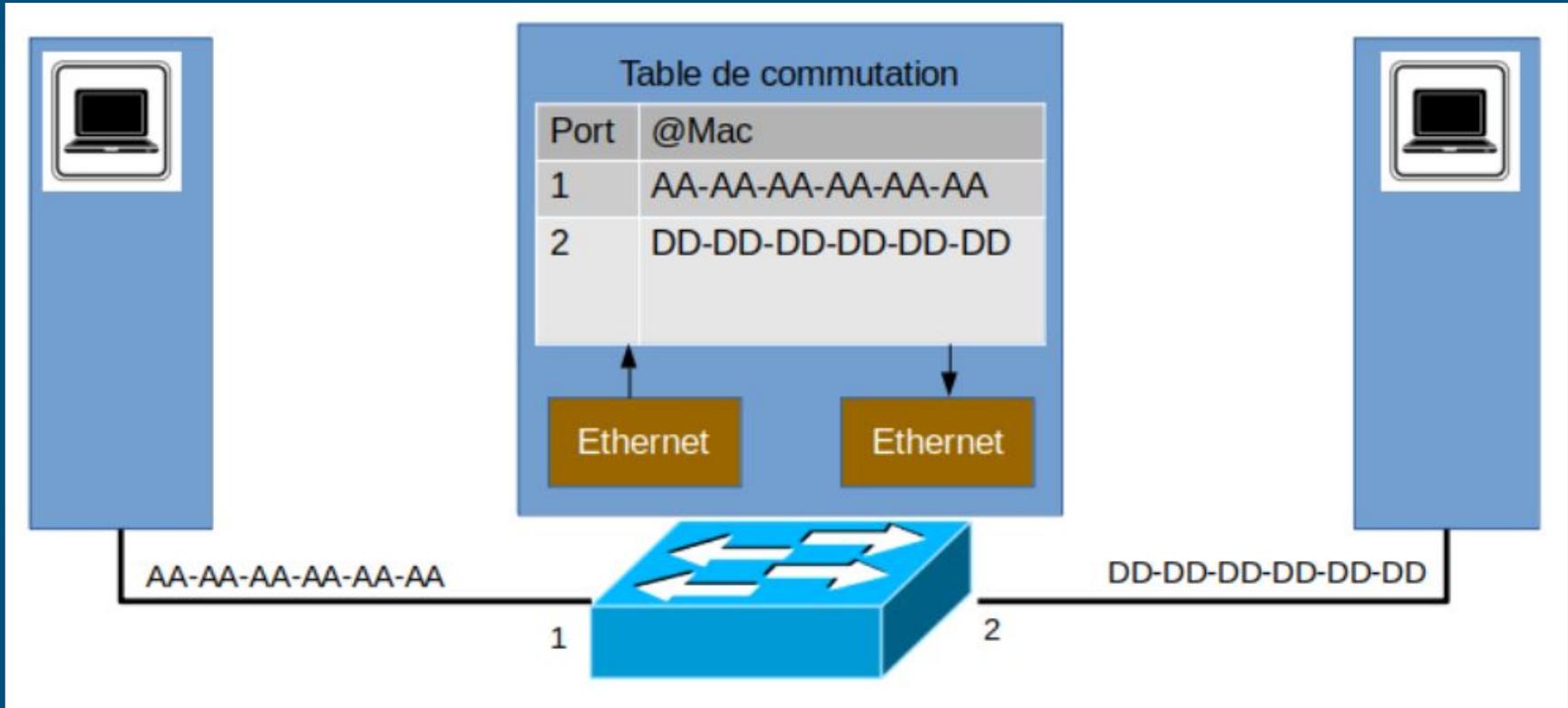
# Un petit exemple



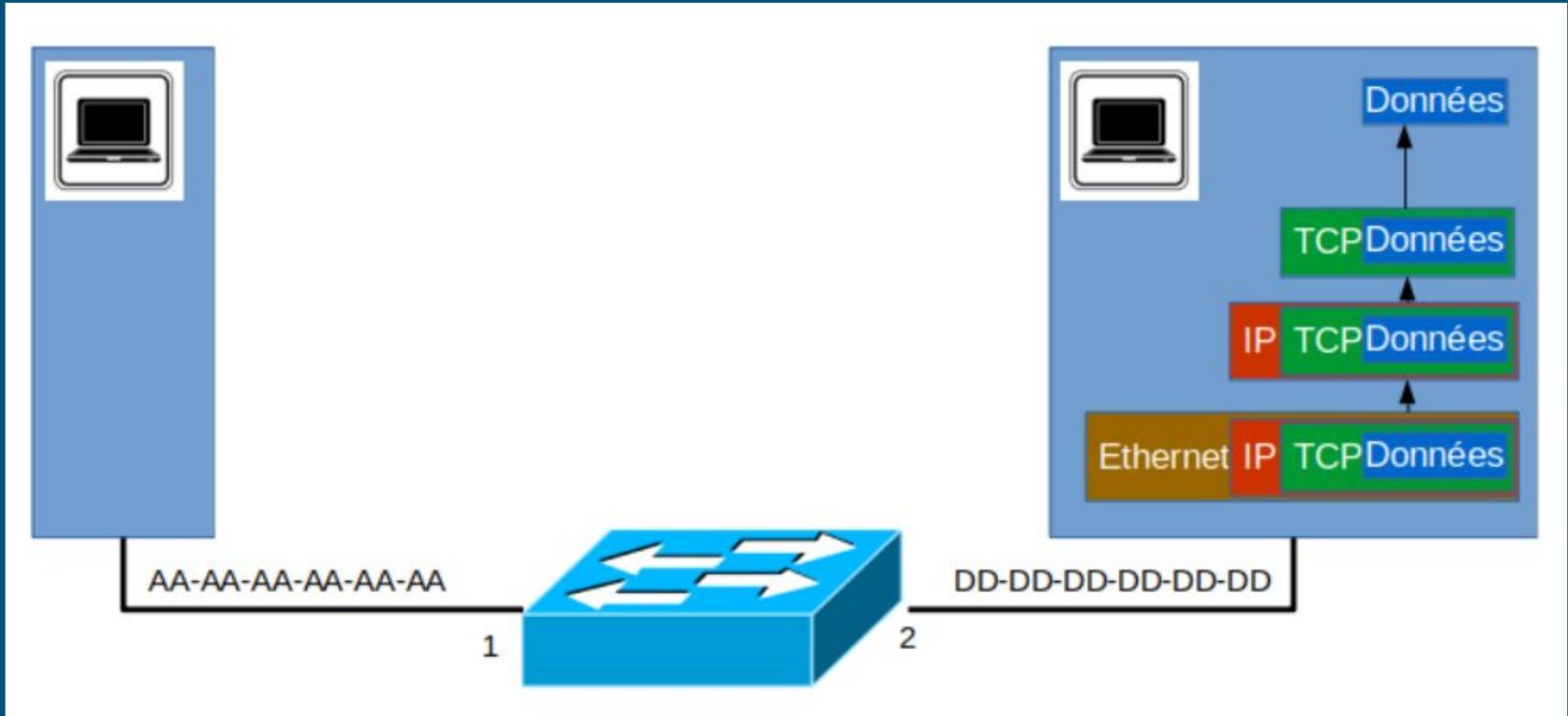
# Un petit exemple



# Un petit exemple



# Un petit exemple



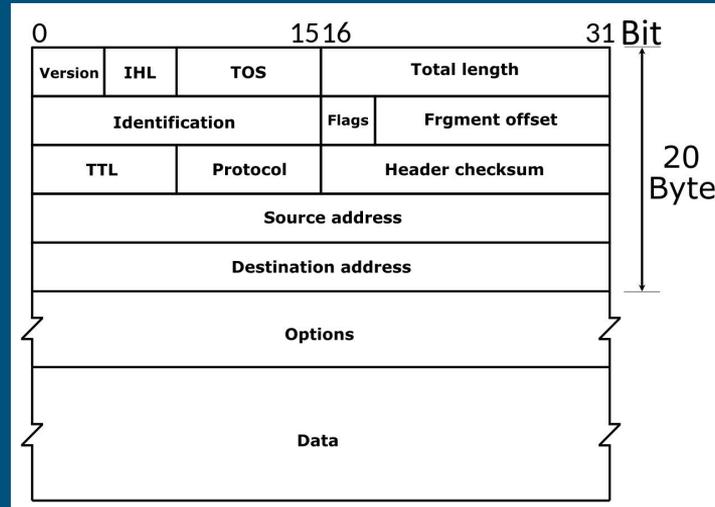
# Allô? J'ai le bon numéro?

---

- Pour faire le lien entre IP et MAC : le protocole ARP
- 2 étapes :
  - Broadcast : Qui a telle IP?
  - Réponse : J'ai telle IP et j'ai telle MAC
- Aucun moyen de vérifier si une réponse a été demandée. On peut donc directement forger les requêtes ARP et se faire passer pour un autre ordinateur : c'est l'ARP spoofing
- On peut ainsi remodeler complètement le réseau et se placer comme centre du réseau et faire en sorte que tout passe par nous
- `nemesis arp -v -r -d interface -S IP_source -D IP_destination -h MAC_expéditrice -m MAC_cible -H MAC_source -M MAC_destination`
- `arp spoof -i interface -t cibles hôte_cible`

# Comment je vais sur Internet dans tout ça?

- IPv4 et IPv6
- IPv4 :
  - Quelques IPs réservées au local : 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- On ne peut vraiment s'attribuer n'importe quelle IP
- Trame IPv4 :



# Avançons masqués

- Internet étant le réseau des réseaux, il y a la notion de réseau qui arrive.
- Comment on définit un réseau et qu'on appartient à un réseau ?
  - Couple IP + masque
  - IP de réseau et IP de broadcast
  - Le masque permet aussi de savoir le nombre d'IP disponibles dans un réseau
- Exemple : 192.168.1.0/24
  - IP de réseau : 192.168.1.0 et masque : 255.255.255.0
  - Le masque permet de retrouver le réseau auquel appartient à une IP :
    - Exemple avec 192.168.1.2 :  $192.168.1.2 \& 255.255.255.0 = 192.168.1.0$

```
11000000.10101000.00000001.00000010
& 11111111.11111111.11111111.00000000
= 11000000.10101000.00000001.00000000
```

# Comment on transporte les données?

---

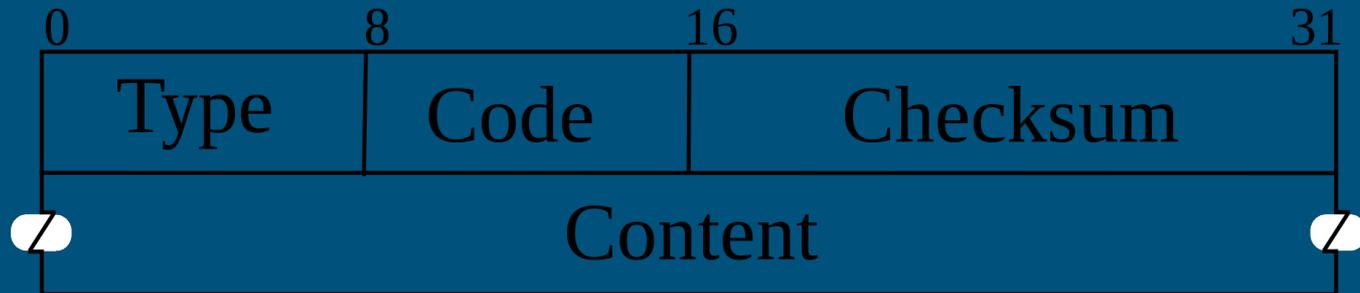
Quatres protocoles principaux :

- **TCP** : garanti l'arrivée des données, qu'elles soient replacées dans le bonne ordre et gère la congestion sur le réseau
- **UDP** : plus léger mais aucune garantie que les données arrivent. Permet aussi de construire son propre protocole de transport par-dessus simplement. Prioritaire sur TCP
- **ICMP** : ping mais aussi message d'erreur
- **QUIC** : nouveau protocole très récent construit sur udp qui apporte le chiffrement au niveau de la couche transport notamment. Principale utilisation : HTTP 3

# Ping? Pong.

---

- Header ICMP :



- Ping of death :
  - Un ping ne peut transporter que  $2^{16}$  octets de données. Sur certaines vieilles implémentations, un ping qui transporte plus de données peut faire crasher la machine

# Allô? Allô, j'ai bien reçu ton allô. Moi aussi, on peut maintenant parler!

- Header TCP :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31								
Port Source 2 octets																Port destination 2 octets																							
Numéro de séquence																																							
Numéro d'acquittement																																							
Taille de l'en-tête				Réservé		ECN / NS		CWR		ECE		URG		ACK		PSH		RST		SYN		FIN		Fenêtre															
Somme de contrôle																Pointeur de données urgentes																							
Options																								Remplissage															
Données																																							

- Attaque DOS par SYN flooding
- On peut aussi détourner un flux TCP en envoyant un drapeau RST puis en interceptant le 3-way handshake TCP
- Peut servir à scanner les ports d'une machine

# La Brique de base

---

- Header UDP

Port Source (16 bits)	Port Destination (16 bits)	Longueur (16 bits)	Somme de contrôle (16 bits)	Données (longueur variable)
--------------------------	-------------------------------	-----------------------	--------------------------------	--------------------------------

- Problème : comme il n'y a aucune mise en place de session, il est très simple à utiliser pour faire des DOS avec des grands facteurs d'amplification :
  - Exemple : faire des requêtes DNS mais rediriger la réponse vers la machine cible
  - DDOS de DynDNS en 2016 : des centaines de milliers de machines ont floodé les serveurs DNS de DynDNS d'un nombre très important de requêtes UDP (~1Tbps) qui ont fini par faire tomber les machines pendant plusieurs heures.

# TCP vs UDP



**Kirk Bater** @KirkBater [Follow](#)

This image is a TCP/IP Joke. This tweet is a UDP joke. I don't care if you get it.

**Thread**  
iamkirkbater and jkjustjoshing

**iamkirkbater**  Aug 23rd, 2017 at 9:37 AM  
in #www

Do you want to hear a joke about TCP/IP?

 7

7 replies

**jkjustjoshing** 5 months ago  
Yes, I'd like to hear a joke about TCP/IP

**iamkirkbater**  5 months ago  
Are you ready to hear the joke about TCP/IP?

**jkjustjoshing** 5 months ago  
I am ready to hear the joke about TCP/IP

**iamkirkbater**  5 months ago  
Here is a joke about TCP/IP.

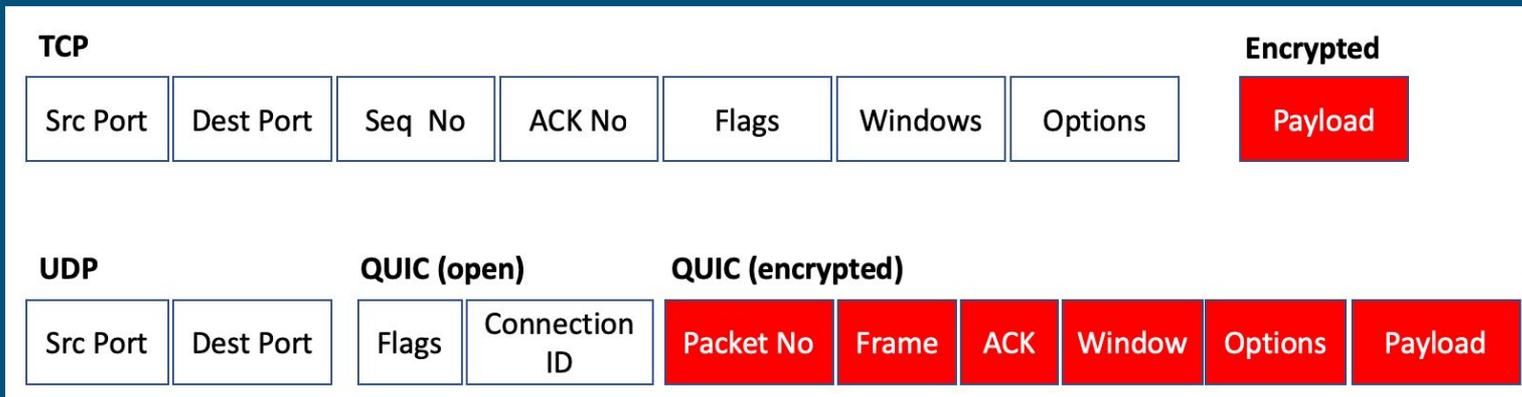
**iamkirkbater**  5 months ago  
Did you receive the joke about TCP/IP?

**jkjustjoshing** 5 months ago  
I have received the joke about TCP/IP.

**iamkirkbater**  5 months ago  
Excellent. You have received the joke about TCP/IP. Goodbye.

# QUIC

- Créé spécialement pour le web et HTTP 3 est construit dessus
- Reprend toutes les propriétés de TCP et rajoute les propriétés suivantes :
  - chiffrement (on dit chiffrer et pas crypter cf chiffrer.info)
  - stream multiplexing
  - latence réduite
  - migration de connexion en cas de changement d'ip



# L'application

---

- Dans la couche application se situent les données qui doivent être transportées et qui nous intéressent.
- Leur format va dépendre du type de données et du protocole utilisé pour les transporter (HTTP, FTP, POP, IMAP, SMTP, DNS, etc.)

Des questions ?