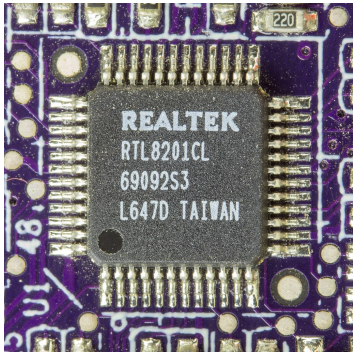
Cours 7

Les Couches Basses

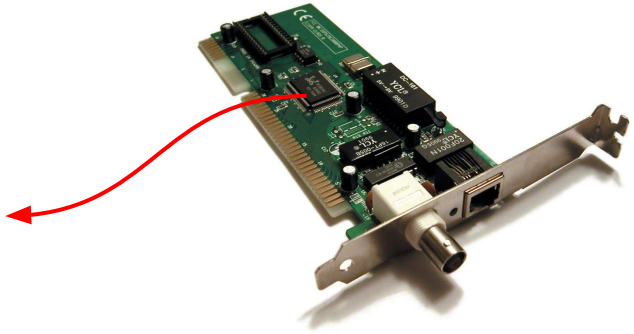
Les Couches Basses

Couche Physique (physical layer)

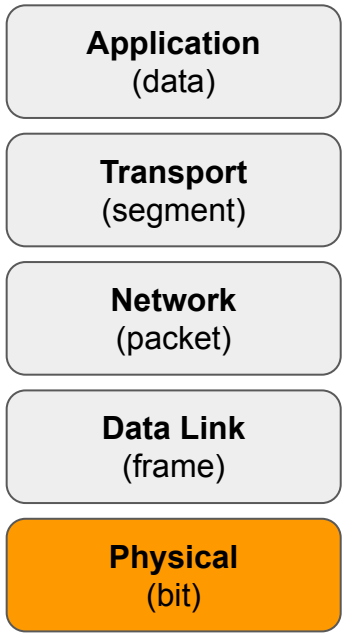
- transmission effective des signaux (électriques, radiofréquences, optiques)
- service typiquement limité à l'émission et la réception d'un bit ou d'un train continu de bits
- réalisé par un circuit électronique spécifique, appelé PHY (*physical transceiver*)



Ethernet PHY



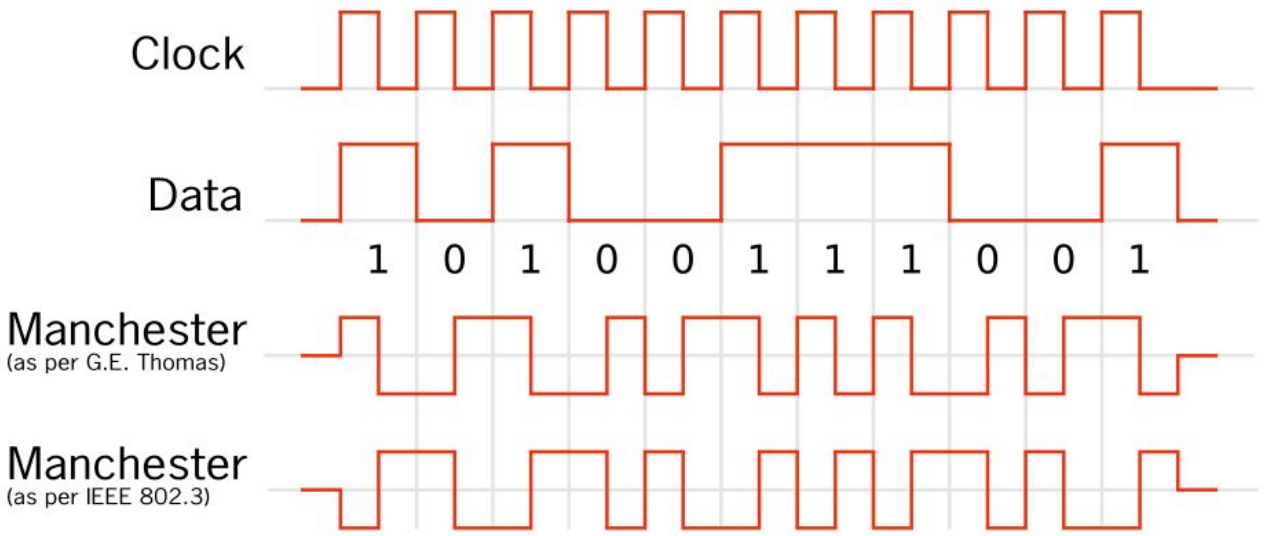
carte réseau Ethernet



Code Manchester

Codage du flux binaire en signaux électrique (couche physique)

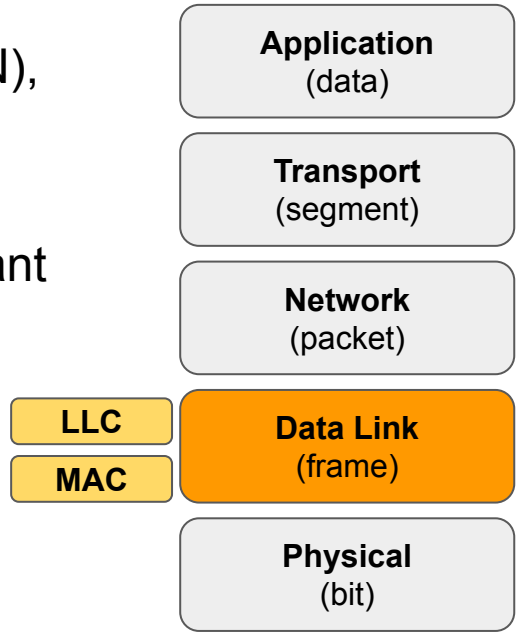
- Ethernet est basé sur le codage Manchester
- tensions -0.85 et +0.85 volts
- approche robuste utilisant une transition pour chaque bit, ce qui facilite la synchonisation ainsi que la détection du début de l'émission

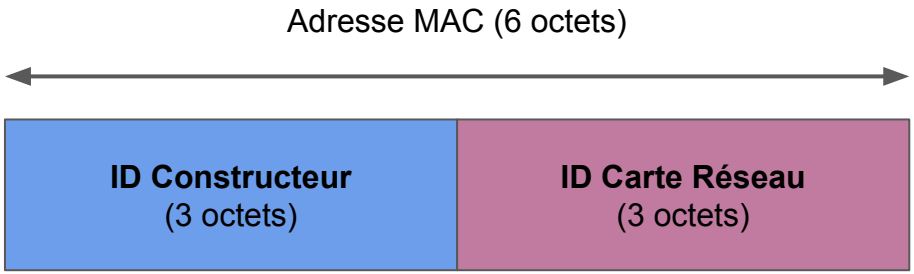


Les Couches Basses

Couche Liaison de Données (data link layer)

- communication entre les noeuds d'un réseau local (LAN), directement reliés par un support physique…
- **LLC** (Logical Link Control) : sous-couche haute
- **MAC** (Media Access Control) : sous-couche basse faisant l'interface avec une couche physique spécifique…
  - détection début & fin de trame, gestion des erreurs (CRC)
  - implantation logicielle ou matérielle sur la carte réseau…
  - adressage MAC : 52:54:00:A1:61:CB





Le Standard Ethernet

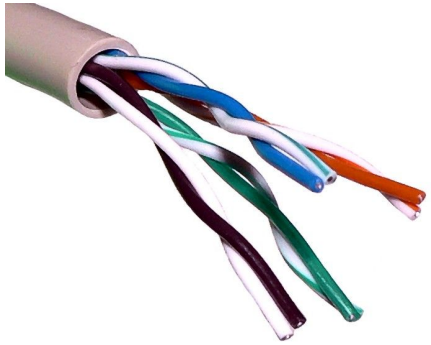
Première technologie LAN grand-public

- inventé au début des années 70 par Xerox, spécifié dans les années 80.
- plusieurs variantes du standard : Ethernet II, IEEE 802.3, …
- évolution du débit : Ethernet (10 Mb/s), Fast Ethernet (100 Mb/s), Giga Ethernet (1000 Mb/s), et plus…

Cablage

- Cable coaxial (10BASE2, 10BASE5)
- Cable UTP : paires torsadées (10BASE-T, 100BASE-TX, …)

cable coaxial



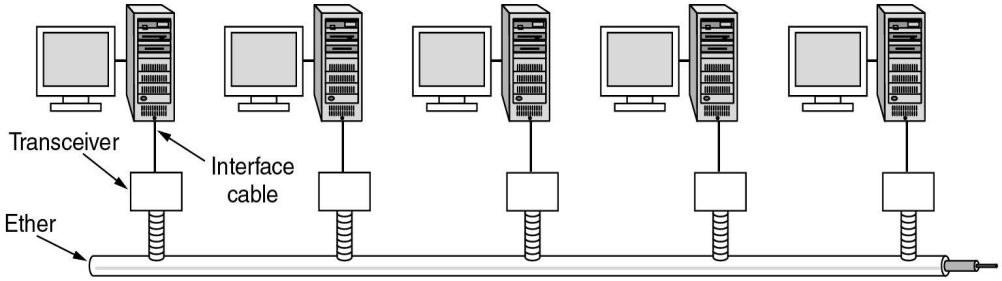
4 paires torsadées

connecteur RJ45

Interconnexion des Machines

Bus

- topologie linéaire, canal partagé
- collision possible des signaux, sujet aux pannes ⇒ désuet



Hub (concentrateur)

- topologie en étoile, half-duplex, canal partagé
- collision possible des signaux ⇒ désuet

Switch Ethernet 5 ports

Switch (commutateur)

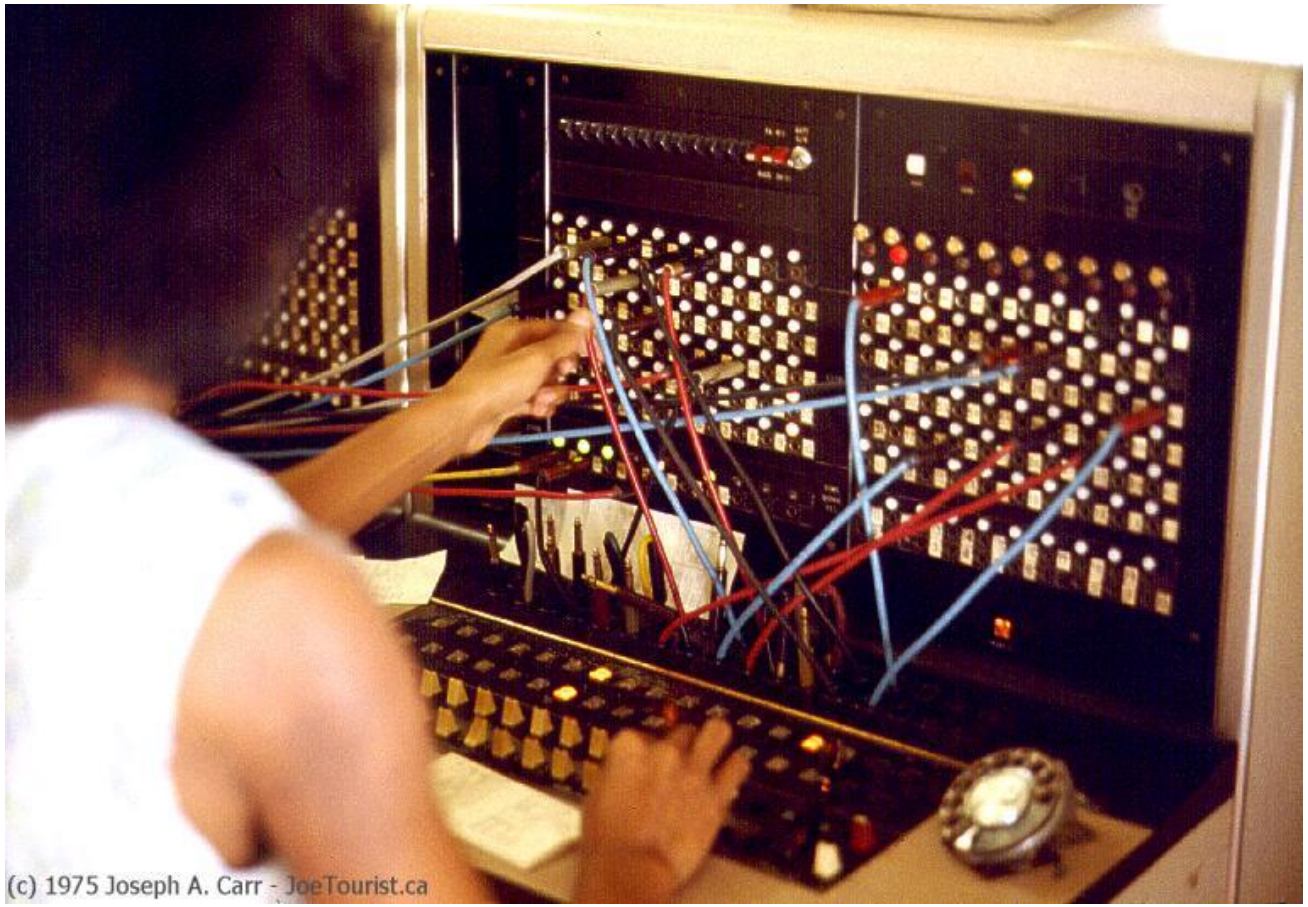
- topologie en étoile, full duplex, canal dédié avec le destinataire choisi (circuit virtuel créé par le commutateur) ⇒ pas de collision

Passerelle / Routeur

- Matériel reliant deux réseaux différents et les faisant communiquer

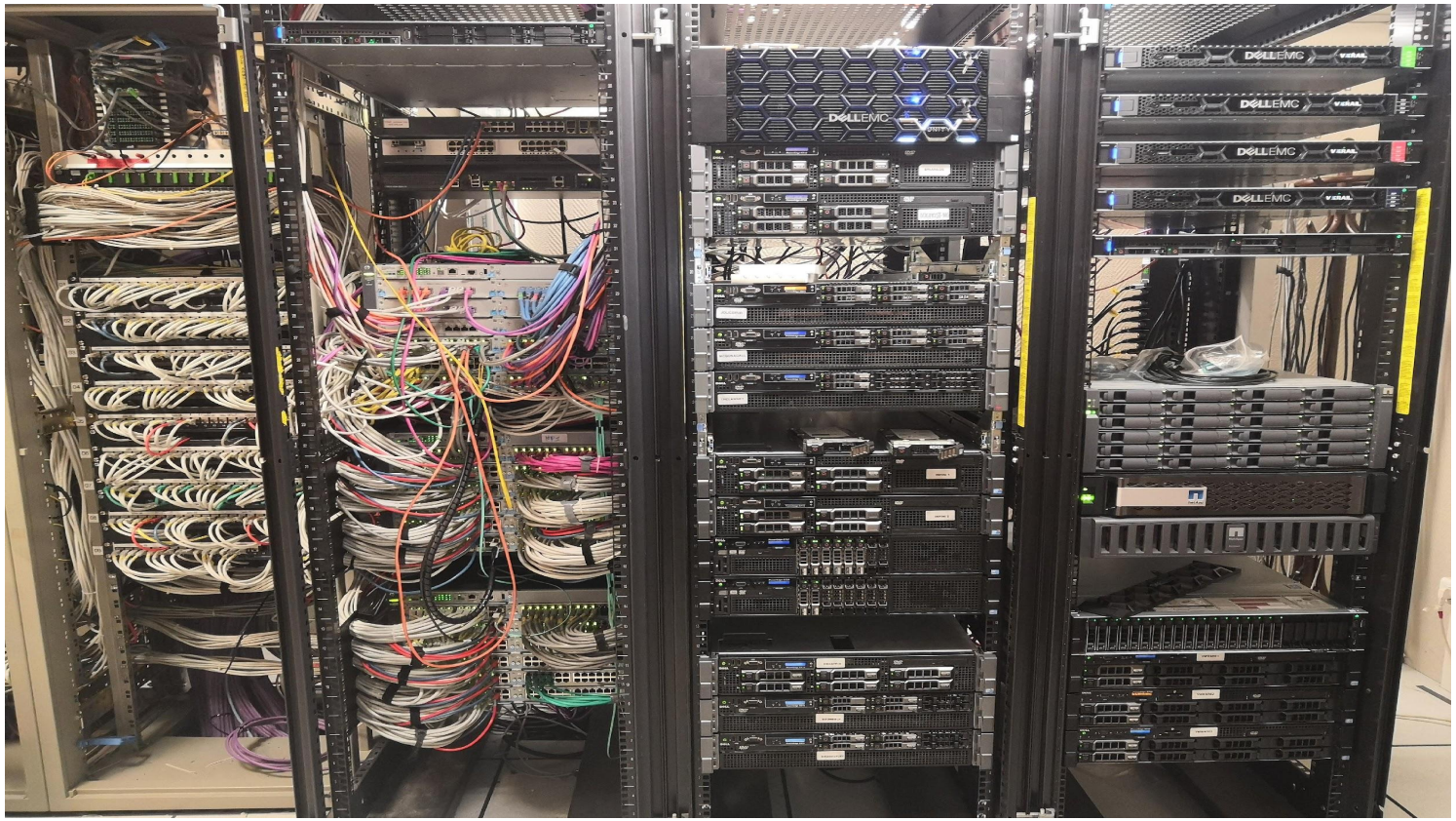
Commutation

Exemple de commutation manuelle sur le réseau téléphonique (RTC)



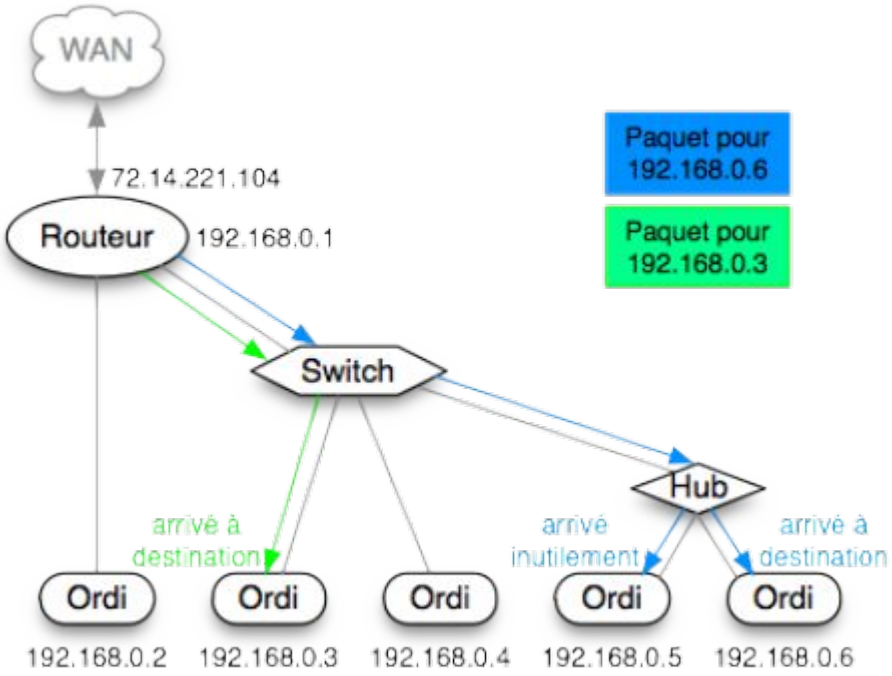
Armoire Réseau

Baie de brassage dans la salle serveur du CREMI.



Interconnexion des Machines

Exemple



Source : http://bencello.net/Tutos.php

Exercice : Au même moment, deux paires de machines communiquent en saturant un réseau Ethernet à 100 Mbit/s. Quel débit maximal peut-on espérer entre chaque machine avec un Hub ou un Switch ?

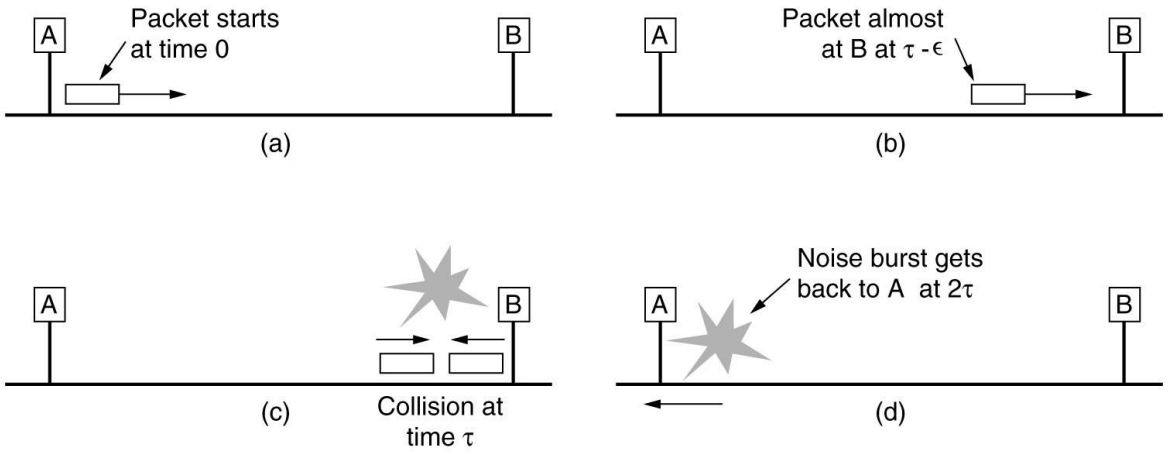
Détection de Collisions

CSMA/CD (Carrier Sense Multiple Access / Collision Detection)

- un seul émetteur à la fois qui monopolise un canal partagé
- écoute de porteuse (carrier) pour sonder si le canal est libre

Principe détection de collision sur le bus Ethernet

- la détection doit se produire lors de l'emission, qui doit durer au moins le temps max d'un aller-retour sur le bus ⇒ taille minimale de la trame
- en cas de collision, réémission avec un délai aléatoire supplémentaire



Exercice CSMA/CD

Calcul de la trame minimale S dans le cas Ethernet (10 Mbit/s)

- D = 10 Mbit/s et d_{max} = 5000 m
- v = 0,70 c = 200 000 km/s (vitesse signal électrique)

La détection de collision doit avoir lieu pendant l'émission, qui doit durer au moins le temps d'un aller-retour...

- $T_{A/R}$ = 2 x (5000 / 200 000 000) = 50 µs

Donc S = $T_{A/R}$. D = 50.10^{-6} x 10.10^{6} = 500 bits = 62,5 octets (au moins)

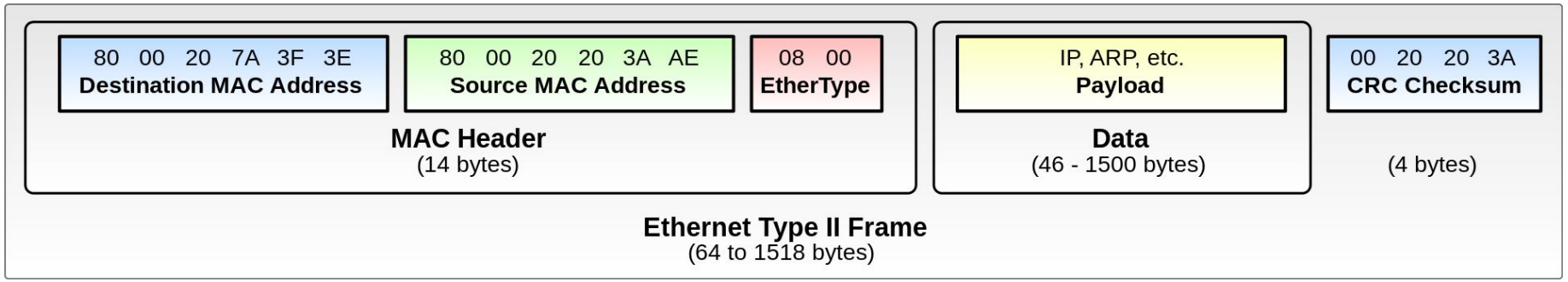
En fait, la valeur minimale de S est fixée à 64 octets.

La taille du paquet IP minimale est donc de 46 octets (avec 14 octets d'en-tête Ethernet + 4 octets de CRC)

Trame Ethernet

Cas du standard Ethernet II

- **Flag Start :** marqueur de début de trame (010101...0101 11) [8 octets]
- **Adresse MAC destination** [6 octets]
- **Adresse MAC source** [6 octets]
- **EtherType** : 0x0800 = IPv4 ; 0x86DD = IPv6 ; 0x0806 = ARP ; … [2 octets]
- **Data :** au minimum 46 octets, jusqu'à 1500 octets (selon MTU), caractères de bourrage (*padding*) si pas assez de données
- **Checksum :** CRC-32 [4 octets]
- **Flag End** : silence à la fin avant la prochaine trame [12 octets]



Exemple d'une Trame Ethernet / IP

Un exemple de trame Ethernet II

```
BB BB BB BB BB BB AA AA AA AA AA AA 08 00  45 00   ..............
00 20 00 01 00 00 40 FF F8 8A C0 A8 00 01 C0 A8   ..............
00 02 48 45 4C 4C 4F 20 57 4F 52 4C 44 21  XX XX   ..HELLO WORLD!..
XX XX XX XX XX XX XX XX XX XX XX XX  ZZ ZZ ZZ ZZ   ..............
```

`Ethernet` / `IP` / `RAW`

Exercice

- Quel est l'adresse MAC de la source et de la destination ?
- Quelle est la taille de cette trame ?
- Quel protocole est encapsulé dans la trame Ethernet ? Détaillez.
- Que repésente les octets `XX` et `ZZ` à la fin ?

Exemple d'une Trame Ethernet / IP

Correction

```
BB BB BB BB BB BB AA AA AA AA AA AA 08 00  45 00   ..............
00 20 00 01 00 00 40 FF F8 8A C0 A8 00 01 C0 A8   ..............
00 02 48 45 4C 4C 4F 20 57 4F 52 4C 44 21  XX XX   ..HELLO WORLD!..
XX XX XX XX XX XX XX XX XX XX XX XX  ZZ ZZ ZZ ZZ   ..............
```

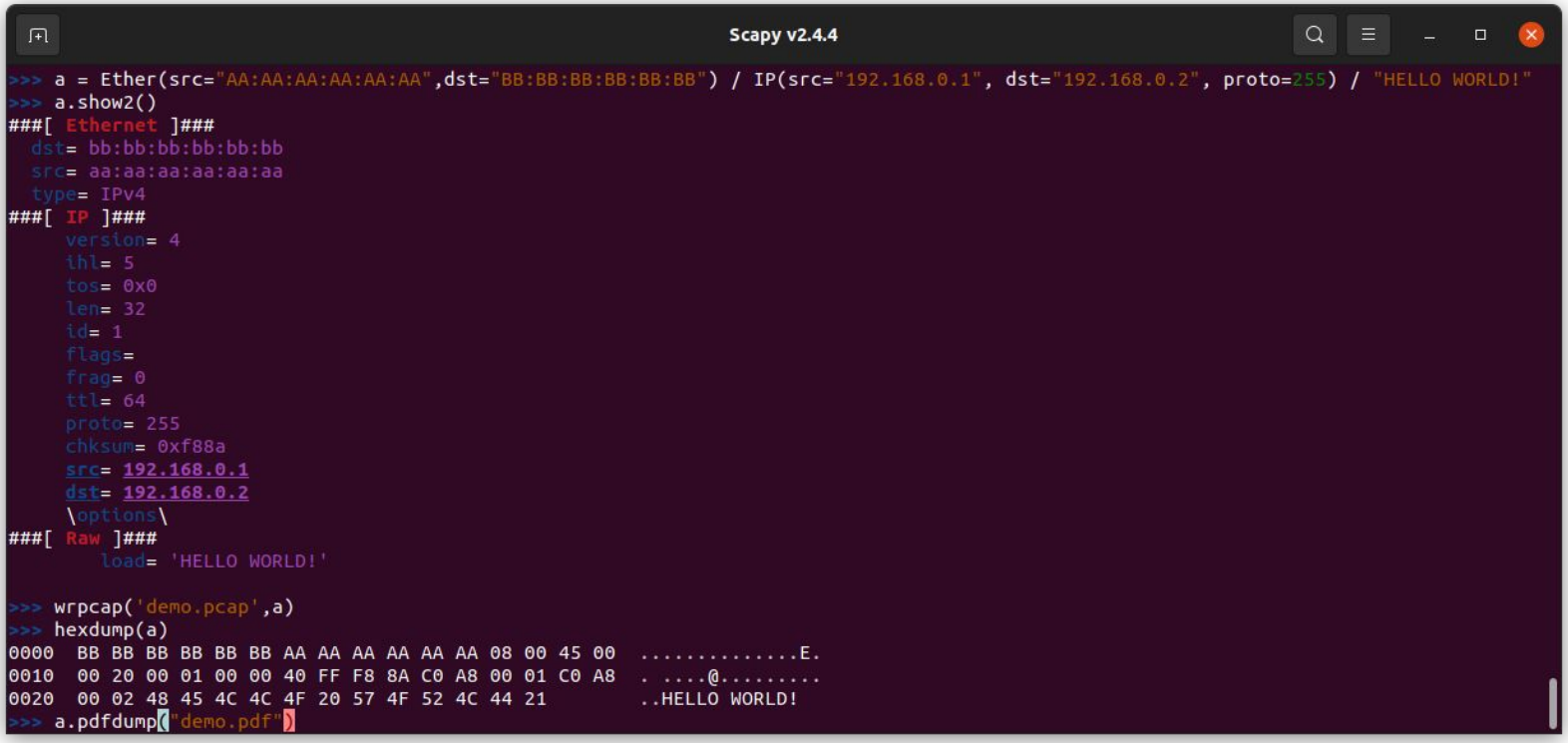
```
Ethernet / IP / RAW
```

- Trame Ethernet de taille minimale 64 octets (4 lignes de 16 octets)
- @MAC source = `AA:AA:AA:AA:AA`
- @MAC destination = `BB:BB:BB:BB:BB`
- Type de protocole : IP (`08 00`)
- L'en-tête du paquet IP nous indique que c'est la version 4 de IP.
- La longueur de l'en-tête est de 20 octets (IHL=5)
- Le paquet IP contient un texte brut `HELLO WORLD!` (12 octets)
- Les 4 octets `ZZ` à la fin sont la checksum CRC.
- Les octets `XX` sont en fait des octets de bourrage (ou *padding*)

Exemple d'une Trame Ethernet / IP

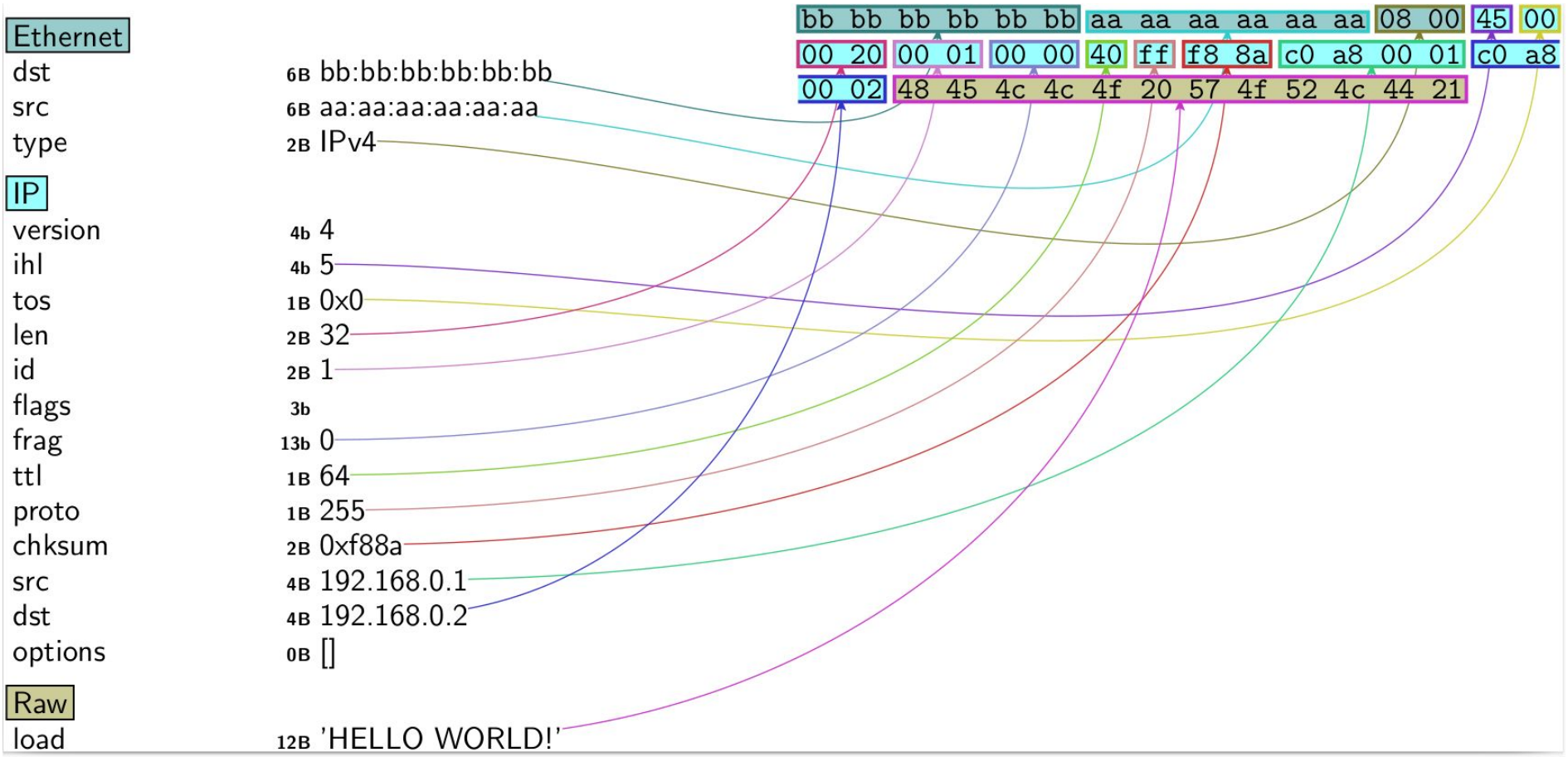
Génération d'une trame "à la main" avec *Scapy3*

```
>>> a = Ether(src="AA:AA:AA:AA:AA:AA",dst="BB:BB:BB:BB:BB:BB") /
IP(src="192.168.0.1", dst="192.168.0.2", proto=255) / "HELLO WORLD!"
```



⇒ https://scapy.readthedocs.io/en/latest/usage.html#interactive-tutorial

Exemple d'une Trame Ethernet / IP



Nota Bene : Il devrait y avoir du *padding* ici, car la trame Ethernet a une taille < 64 octets. On ne voit pas non plus le CRC. En fait, ces informations sont calculés et ajoutés automatiquement dans la trame Ethernet au moment de l'envoi par la carte réseau.

ARP

Problèmatique : Au sein d'un réseau local, les adresses MAC sont utilisées pour communiquer entre les machines (trame Ethernet). Mais comment découvrir l'adresse MAC du destinataire ?

ARP (Address Resolution Protocol) : protocole de résolution des adresses MAC à partir des adresses IP, RFC 826.

- La source diffuse la requête ARP "WHO HAS @IP?" en broadcast Ethernet dans le réseau local (FF:FF:FF:FF:FF:FF)
- La machine @IP répond avec son @MAC
- La machine source enregistre le résultat dans le cache ARP

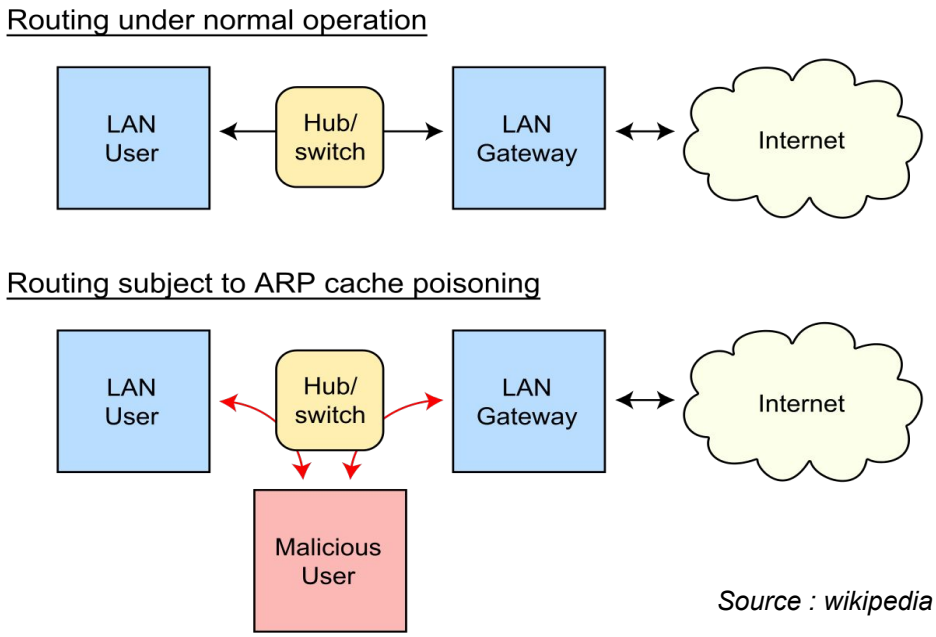
Outils : affichage du cache ARP

```
$ arp -n
(192.168.2.109)   00:23:69:15:28:51 [ether] wlan0
(10.20.30.100)    00:22:19:dd:0b:65 [ether] eth0
```

ARP Spoofing

Mise en place d'une attaque du type "Man-in-the-Middle"

- Empoisonnement du cache ARP de 2 machines victimes pour détourner les trames Ethernet vers la machine de l'attaquant…
- Envoi continu par l'attaquant de réponse ARP frauduleuse…



Source : wikipedia

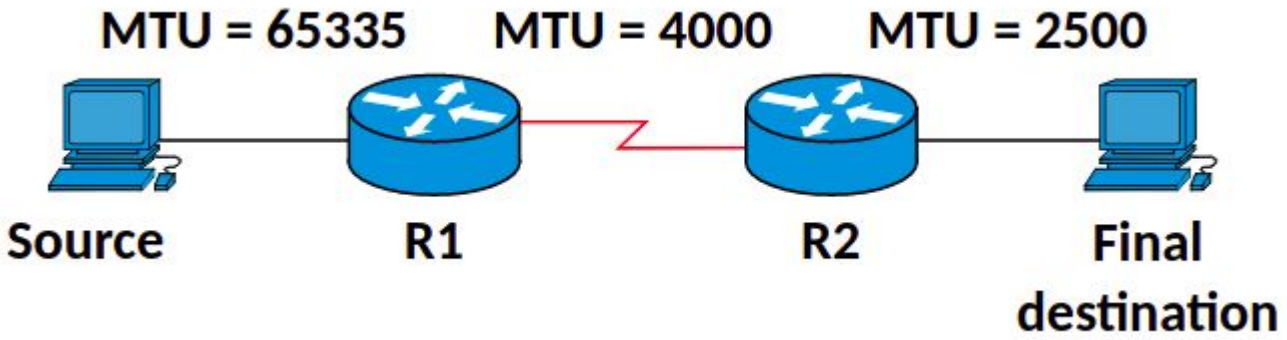
MTU

MTU (Maximum Transmission Unit)

- Taille maximale du paquet IP sur un lien physique (1500 octets sur Ethernet)
- **Path MTU** : plus petite MTU sur le chemin d'un paquet IP

Path MTU discovery

- Découverte du Path MTU entre la source et la destination
  - envoi d'un paquet IP avec le flag DF (Dont Fragment) ⇒ erreur MTU si paquet trop grand !
- Outils : `tracepath <dest>` ou `traceroute --mtu <dest>`



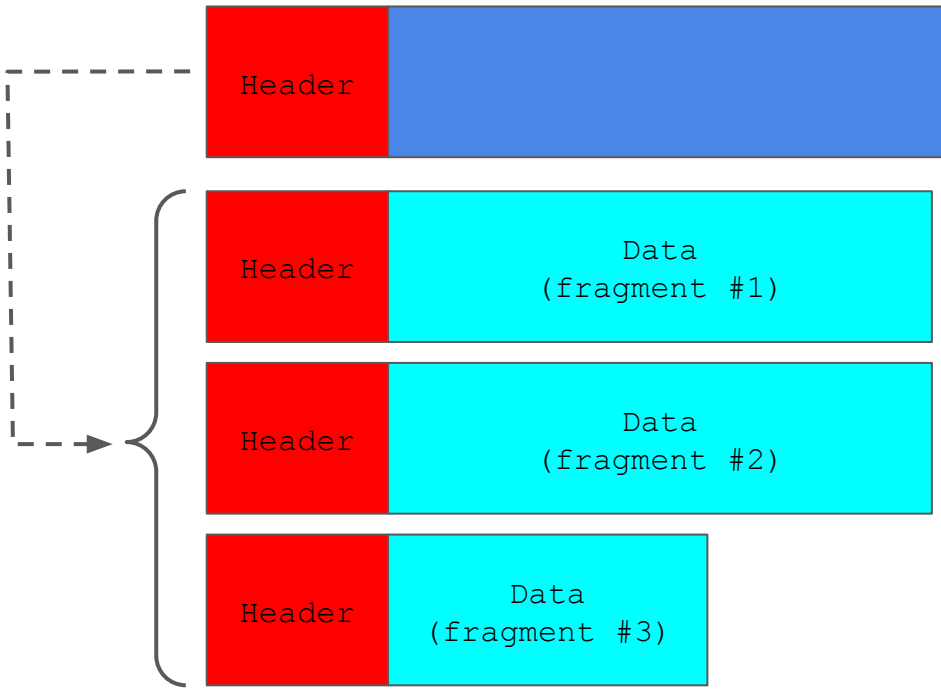
Exercice : Quel est la valeur du *Path MTU* ?

Fragmentation d'un Paquet IP

Fragmentation

- Découpage des paquets IP en plusieurs fragments pour ne pas dépasser la MTU…
- Numérotation des fragments composant le paquet initial…

Exemple : fragmentation d'un paquet de 4000 octets (MTU=1500)



Exercice : Quel est la taille des différents fragments ?

Paquet = Header + Data = 20 octets + 3980 octets

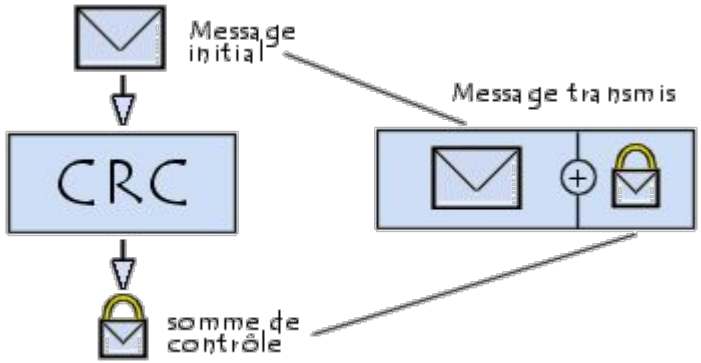
Fragment #1 = 1480 octets
Fragment #2 = 1480 octets
Fragment #3 = 1020 octets

Checksum CRC

Code CRC-N de clé K (sur N bits) : Calcul de *checksum* basé sur une méthode de division binaire (avec *xor*) par G=(1|K) sur N+1 bits. Le code CRC est le reste de la division R, réprésenté sur N bits.

Plus précisément :

- Soit Z=0x0 sur N bits. On pose la division (M|Z) / G pour calculer le reste R.
- Puis, on envoie le message M'=(M|R).
- On reçoit le message M'', qu'on espère identique à M'. Pour le vérifier, on pose la division M'' / G et on vérifie que le reste R'=0x0.

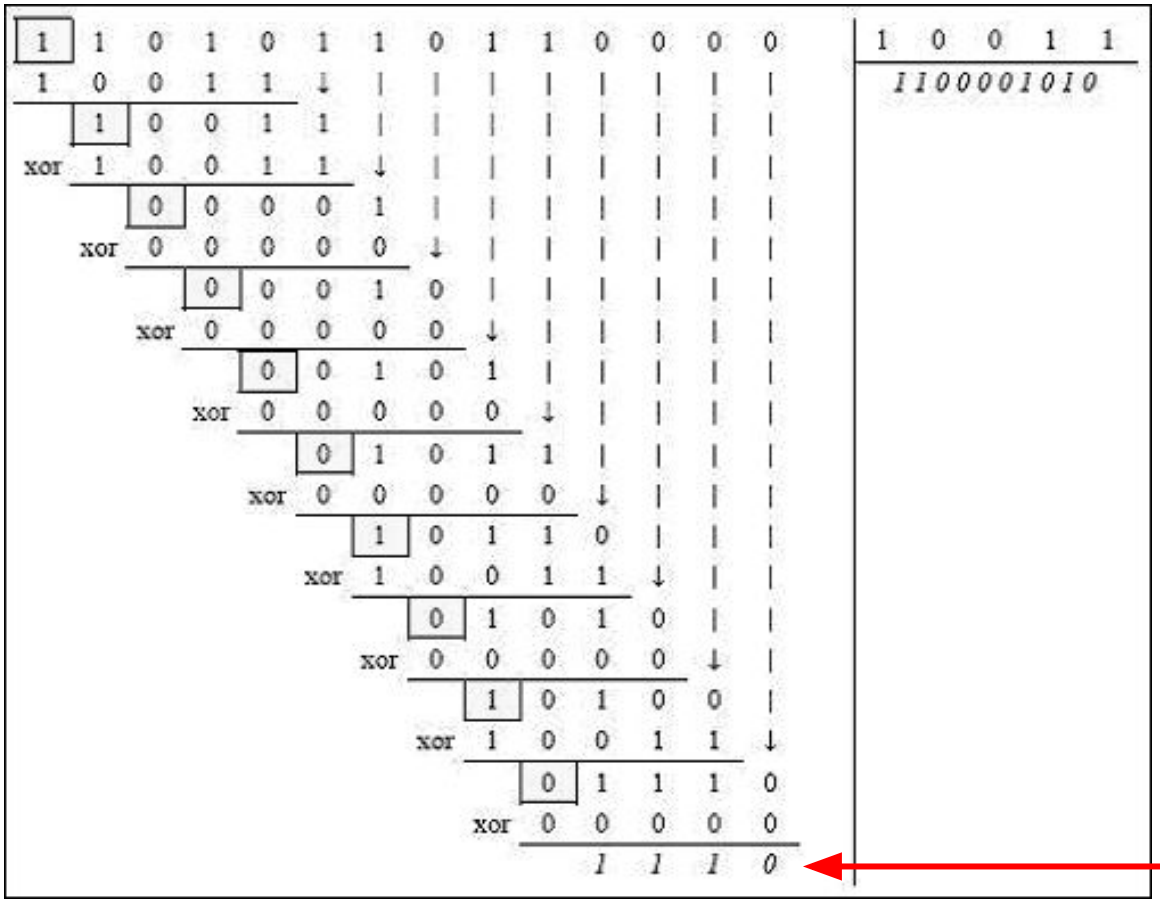


Source : https://www.commentcamarche.net/

Checksum CRC

Exemple de CRC-4 avec K=0x3.

Considérons le message M=1101011011. On a N=4, K=0011 et G=10011. On pose la division 11010110110000 / 10011. Le résultat est le reste R=1110 (4 bits).



Checksum CRC

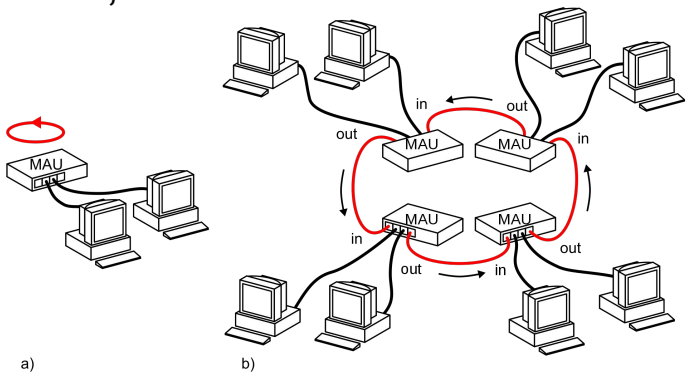
Quelques exemple de CRC standards :

- CRC-1 avec K=0x1 (bit de parité)
- CRC-8 avec K=0x07 (ATM)
- CRC-8 avec K=0xA7 (Bluetooth)
- CRC-16 avec K=0x8005 (USB)
- CRC-32 avec K=0x04C11DB7 (Ethernet)
- CRC-40 avec K=0x0004820009 (GSM)

Une Grande Variété de Technologies

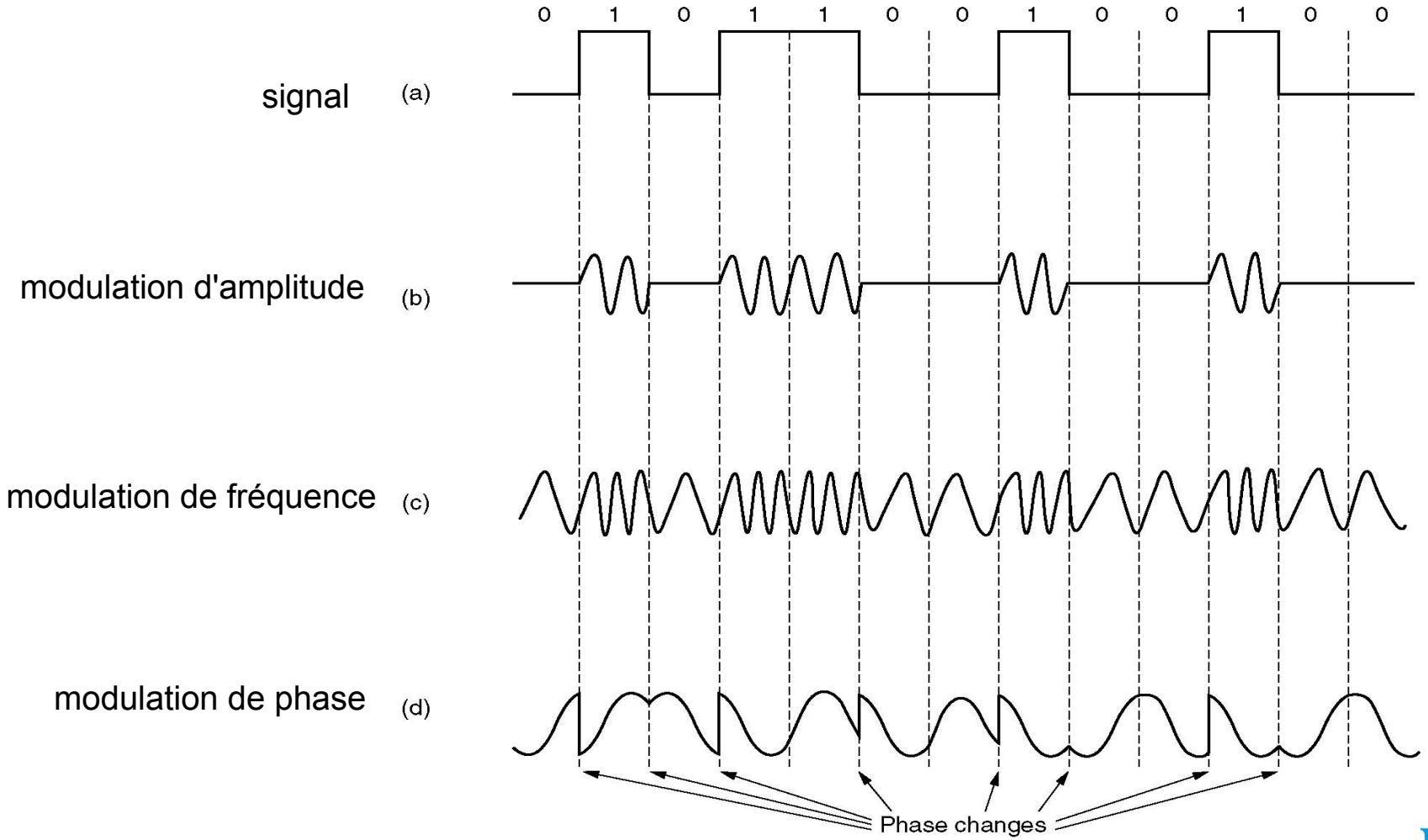
Une séparation pas souvent très claire entre les couches basses !

- **Token Ring** : topologie en anneau, jeton (trame de 3o) qu'il faut passer à son voisin pour qu'il puisse commencer à émettre…
- **FDDI** (Fiber Distributed Data Interface) : mise en oeuvre d'un double anneau à jeton avec la fibre…
- **ATM** (Asynchronous Transfer Mode) : transmission des données par cellules de tailles fixes, très répandu au coeur du réseau ADSL !
- **V.90** : protocole physique utilisé par les modems téléphoniques 56K
- **Wi-Fi** (IEEE 802.11) : variante sans fil d'Ethernet ou *Wireless* LAN
- **PPP** (Point-to-Point Protocol), **SLIP** (Serial Line Internet Protocol), **FTTH** (Fiber to the Home), **ADSL**, …



Transport du Signal Numérique

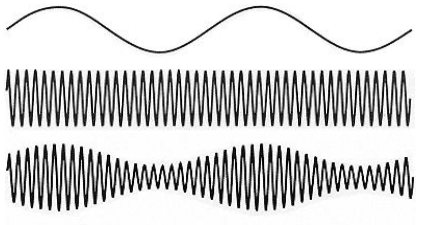
Différentes techniques de modulations autour de la fréquence d'une porteuse (*carrier*)



Quelques Exemples

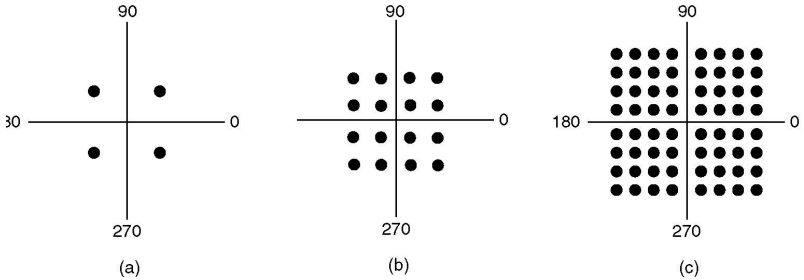
Modulation d'amplitude

- radio AM, TV Hertzienne, …



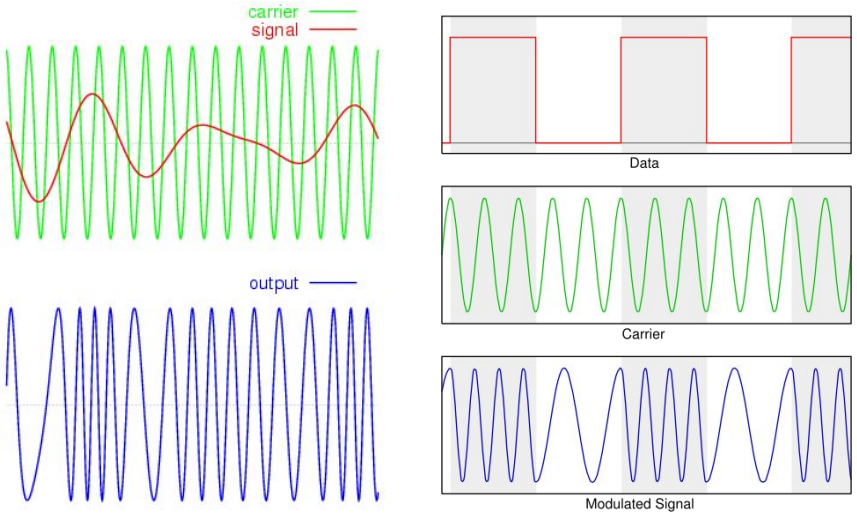
Modulation de phase et d'amplitude

- Modem V.90, ADSL, Wi-Fi, …



Modulation de fréquence

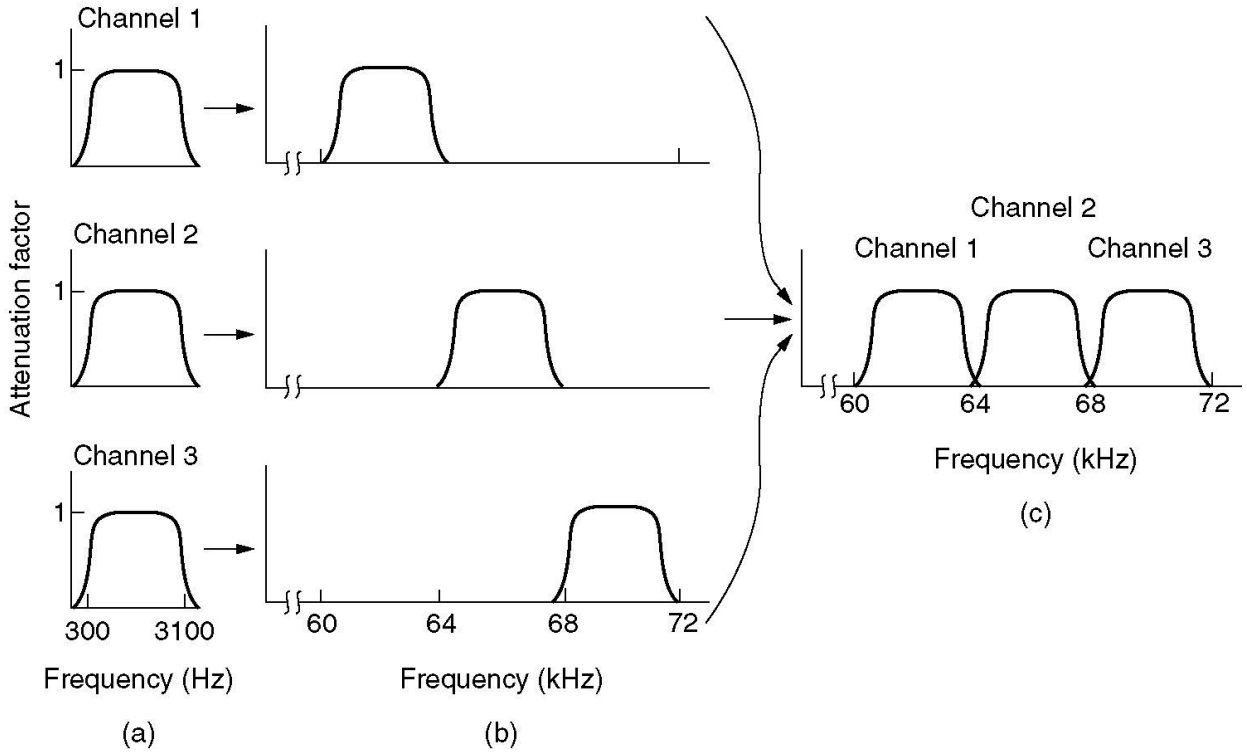
- radio FM, GSM, …



Multiplexage Fréquentiel

Transmission simultanée en utilisant de multiples channels

- Division de la bande de fréquences en channels (plusieurs sous-porteuses)
- Exemples : TNT, ADSL, Wi-Fi, …



Wi-Fi

Réseaux locaux sans fil (Wireless LAN ou WLAN)

- Interconnexion des objets connectés par onde radio…
  - Bandes de fréquence 2.4 / 5 GHz avec une portée max entre 10 & 100 m
- Norme IEEE 802.11 (à partir de 1997)
  - Historiquement, Wi-Fi signifie *Wireless Fidelity*, ce qui est en fait la certification du respect de la norme 802.11
- Les différentes générations de Wi-Fi

Generation/IEEE Standard	Maximum Linkrate	Adopted	Frequency
Wi-Fi 6E (802.11ax)	600 to 9608 Mbit/s	2019	6 GHz
Wi-Fi 6 (802.11ax)	600 to 9608 Mbit/s	2019	2.4/5 GHz
Wi-Fi 5 (802.11ac)	433 to 6933 Mbit/s	2014	5 GHz
Wi-Fi 4 (802.11n)	72 to 600 Mbit/s	2008	2.4/5 GHz
802.11g	6 to 54 Mbit/s	2003	2.4 GHz
802.11a	6 to 54 Mbit/s	1999	5 GHz
802.11b	1 to 11 Mbit/s	1999	2.4 GHz
802.11	1 to 2 Mbit/s	1997	2.4 GHz

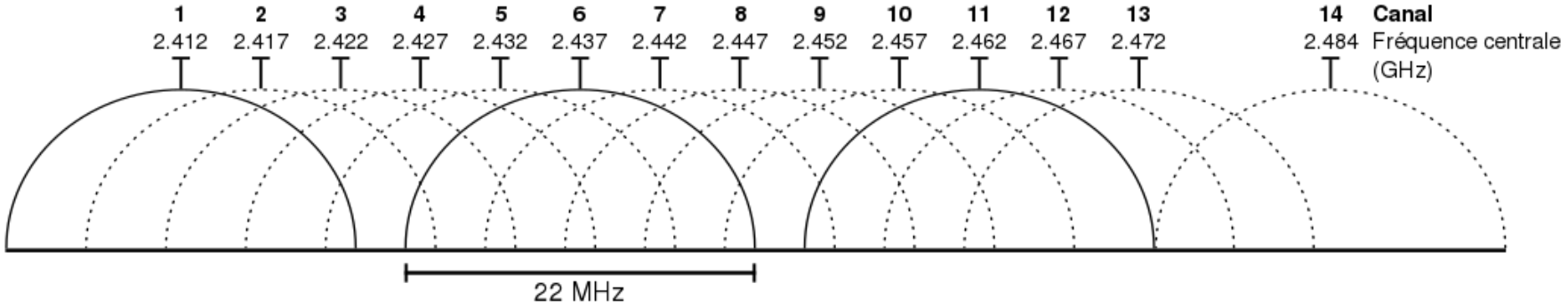
Exemple de routeur Wi-Fi NetGear

Wi-Fi

Les couches basses du Wi-Fi

- Couche Physique : modulation amplitude & phase sur un channel (QAM)
  - En Wi-Fi 6, multiplexage fréquentiel (OFDM) entre plusieurs utilisateurs
- Couche Liaison : proche du standard Ethernet (MAC, LLC)

Channel : découpage de la bande de fréquence en plusieurs canaux de 22 MHz



⇒ Démo avec un radar wifi...

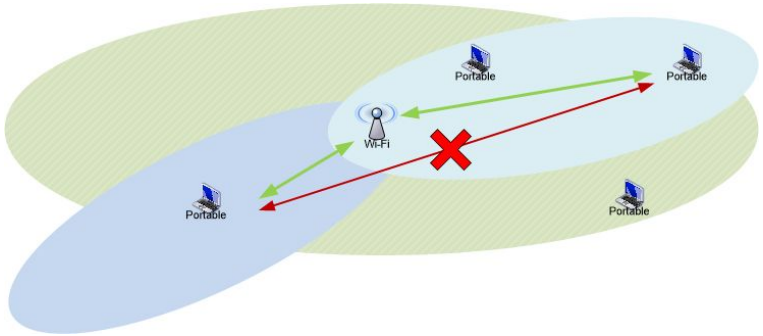
Wi-Fi

Mode Infrastructure

- SSID (Service Set IDentifier) : identifiant du réseau
- AP (Access Point) : la borne qui interconnecte toutes les machines du réseau, passage obligé…
- Securité : WEP, WPA, WPA2, …

Collision Avoidance (CSMA/CA)

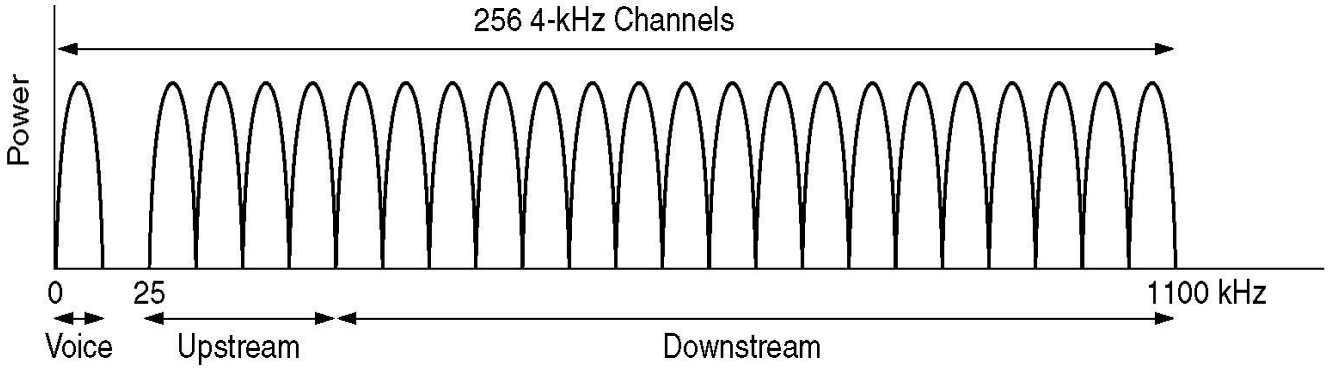
- Pas possible de faire de la détection de collision (CSMA/CD), car les machines qui communiquent peuvent être hors-portée !
- Le point d'accès centralise et arbitre les échanges...



ADSL

ADSL (Asymetric DSL)

- Multiplexage fréquentiel avec 255 channels (sous-porteuses)
- ADSL 1 (< 1.1 MHz) et ADSL 2+ (< 2.2 MHz)
- Multiplexage fréquentiel : division en 255 canaux de 4.3 kHz
- Modulation QAM-250 en parallèle pour chaque canal
- Répartition asymétrique des canaux pour l'envoi et la réception
  - 80 à 90% des canaux en flux descendant ⇒ débits montants et descendants asymétriques
- Débits
  - ADSL, ADSL 2+ (de 1 à 15 Mb/s)
  - VDSL (de 15 à 50 Mb/s), VDSL2 (100 Mb/s)
- Atténuation du débit en fonction de la distance au DSLAM



ADSL

DSL (Digital Subscriber Line)

- Invention en 1988 (Bell), puis essor en France en 1999…
- Utilisation du réseau de téléphonie (RTC) pour transporter 2 flux…
  - Flux analogique sur les fréquences vocales (< 3 400 Hz) : téléphone / Fax / Modem V.90
  - Flux numérique sur les fréquences hautes (DSL)
  - Séparation des deux flux avec un filtre (boitier blanc)
- Connexion du Modem DSL au DSLAM (Access Multiplexer), puis au réseau du FAI (Fournisseur Accès Internet)