# Modèle OSI :

* Avantage :
* les couches communiquent uniquement entre elles
* les technologies d’une couche sont remplaçables

TCP/IP :

raisons de création : besoin de standardiser la communication entre les machines

Avantages :

* Optimisation de la bande passante
* utilisation de plusieurs chemin pour transmettre paquets → réseau robuste

HUB :

Avantage du hub :

* Possible de communiquer avec les PC connectés, de voir l'état des ports, les paquets, etc

→ Matériel actif (avec de l’intelligence)

* Possibilité
* Flexible et extensible
* Câblage indifférencié

# Ethernet :

MAC : Medium Access Control

| Num constructeur | Adaptateur |
| --- | --- |

Longueur de la trame : 1512 octets

Preambule : 64 bits → sert à synchroniser la réception (métronome alternant 1 & 0)

Adresse de destination (MAC) : 48 bits

Adresse source (MAC) : 48 bits

Type: 16 bits

* Type/longueur (DIX, 802.3)

Data :

* Paquet
* IP

FCS : 32 bits (c’est la queue de la trame, pour traiter les erreurs)

Half Duplex :

Canal comme talkie walkie, sois ecouter sois parler, mais pas les 2

CSMA/CD

Carrier Sense Multiple Access / Collision Detection

Etape 1 :

* il écoute la porteuse
  + Ca parle (comparateur)
  + Ca parle pas (j'émets ma trame)

Etape 2 :

* Pendant toute la transmission, je compare Tx (transmission) et Rx (la réception) :
  + Tx = Rx je continue
  + Tx != Rx y’a un abruti qui émet ⇒ Collision Detection

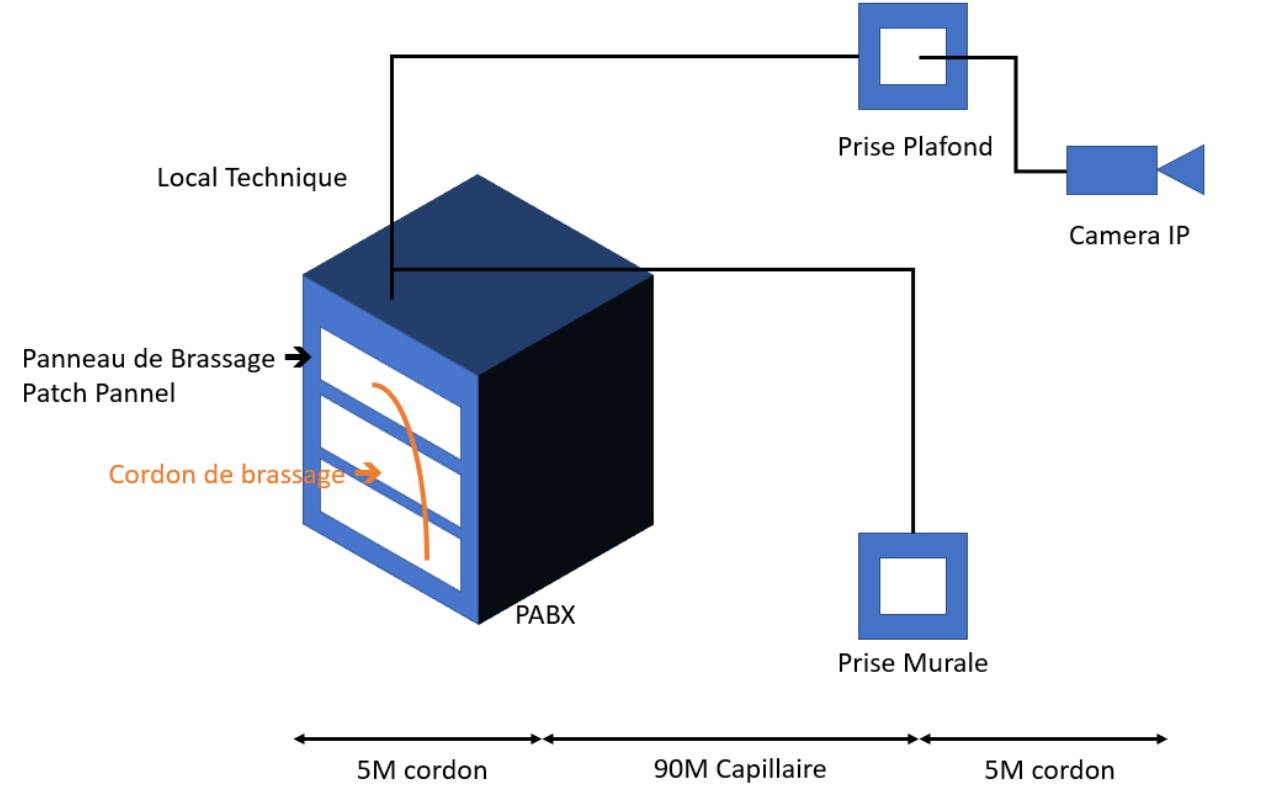
Etape 3 :

* Jamming (je préviens tout le monde)
* J’attend un temps aléatoire et je recommence à l’étape 1

# Cablage

Durée de vie du câblage : 20 à 25 ans

Baie 19 pouces :



Possibilité d’avoir un câblage capillaire supérieur à 90 mètres mais il y a des soucis :

* Non respect norme longueur câblage capillaire → galère pour le changer
* Détérioration de la qualité du signal ← bruits + qualité du cable (cuivre)

longueur → + bruits → qualité plus faible

UTP → Unshielded Twisted Pair

STP → Shielded TP

FTP → Foiled TP

SFTP →

FZTP → Câble émetteur, chaque paire a un écran, et autour de toutes les paires il y a un écran

UFTP → Câble émetteur

Blindage = plein de petits fils tressés, pour les signaux basse frequences (220v)

Ecrantage = protection contre les hautes fréquences

Haute fréquence : effet de Po -> utilisation d’un feuillard (écran)

Catégorie 5 (Classe D = Fonctions)

⇒ 100 MHz et Fast Ethernet (100 Mbits/s)

⇒ Utilisation de 2 paires

Catégorie 5E (Standard)

⇒ 100 MHz et GigaBits Ethernet (1000 Mbits/s)

Categorie 6 (Classe E)

⇒ 250 MHz et GigaBits Ethernet (1000 Mbits/s)

Catégorie 6A (Classe F)

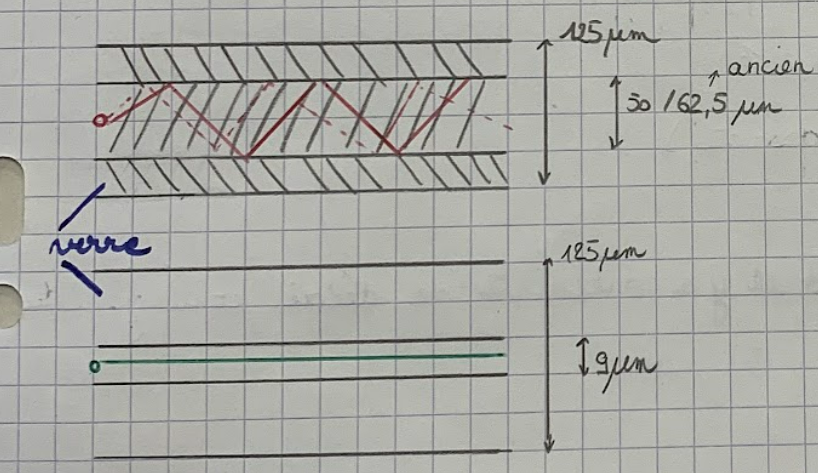
⇒ 600 MHz et 10 GigaBits Ethernet (10 000 Mbits/s)

Règle primordiale lors d’un chantier : Respecter les règles de pose

Fibre optique performante pour 3 raisons :

* + de longueur
* immunité électromagnétique (imperturbable)
* taux d’erreur très faible

Fibre :



Fibre multimode :

Plusieurs chemises ⇒ Distance plus faible

Fibre monomode

# Bridge :

Avantages :

* Plus de PC
* Plus de trafic
* Plus de collision

Défauts :

* Moins de bande passante

⇒ Moins de trafic

2 cas de fonctionnement :

* Unknown Address
  + Flooding
    - Le bridge envoi la trame sur tous ses ports sauf le port source
* Adresse dans la CAM Table
  + Envoi sur le port correspondant si != du port source
* Broadcast
  + Flooding

SPOF : Single Point Of Failure

redondance → plusieurs chemins → boucles

problèmes = comment avoir un chemin unique vers chaque segment Ethernet

les switchs doivent communiquer entre eux

spanning tree

Bloquer une boucle → Spanning Tree

Etapes (Spanning tree) :

1 - Blocage de tous les ports

2 - Election du root bridge (la racine de mon arbre)

1 - Chaque switch envoie une BPDU (Bridge Protocol Data Unit) sur chacun de ses ports

2 - Chaque BPDU contient le Bridge ID ( 16 bits de bridge priority et 48 bits addr MAC)

3 - Chaque switch relance les trames reçues de ses voisins

4 - S’il reçoit une BPDU “meilleure” (+ petite) il arrête d’émettre

5 - Seul le root bridge continue

1 - Election Root Bridge → OK

2 - Root Port → Qui vont “vers le root” } Champ “Port priority” → Path cost

Designated Port → Qui “retient” au root }

Fin - Tant que le switch reçoit la meilleure BPDU sur son root port, il ne fait rien. Si la BPDU n’arrive pas, risque de boucle : on recommence

Diamètre Spanning Tree : 8

→ Nb max de saut possible

4 Piliers de la sécurité :

* Disponibilité
* Intégrité
* Légitimité
* Non Répudiation = non réfutable / Contrôle de la preuve

Nécessite topologie sans boucles

Topology Change Notification

Avantages et inconvénients de chaque structure

BUS → simplicité, prix, pas de redondance, bande passante

BOUCLE → simplicité, prix, bande passante extensibilité

ETOILE → extensibilité, bande passante, SPOF, prix, complexité

ETOILE REDONDANTE → extensibilité, redondant, prix, complexité

# IP

Différence entre adresse IP et adresse MAC :

L’adresse IP est universelle, on peut contacter tout le monde contrairement à l’adresse MAC qui ne peut voir et communiquer qu’avec les machines sur le même réseau.

Route de broadcast 255.255.255.255

Route par defaut (Default Gateway) 0.0.0.0

ARP : Adress Resolution Protocol

Permet de demander des services à la couche 3 depuis la couche 2

Table ARP : Contient correspondance @Mac et @IP

→ Temps de stockage de cette table : 14400s (4 heures)

Mon PC → ARP Request

Adresse de dest : Brodcast (FF:FF:FF:FF:FF:FF)

Qui a l’adresse de destination ( Mise dans la partie Data de la trame)

→ ARP Reply

Internet = réseaux de réseaux

1. Respect des protocoles → ITEF
2. Gestion des adresses → WHOIS → RIPE
3. Gestion des noms de domaine → ICANN → AFNIC

Etape :

1. Boot → POST → Vérification du Hardware
2. ROM MOW → Secteur de boot de l’OS
3. Lire la config (STARTUP)
4. Lancer le binaire
5. Copier la STARTUP en Ram
6. Interprète la config en RAM → devient la Running Config