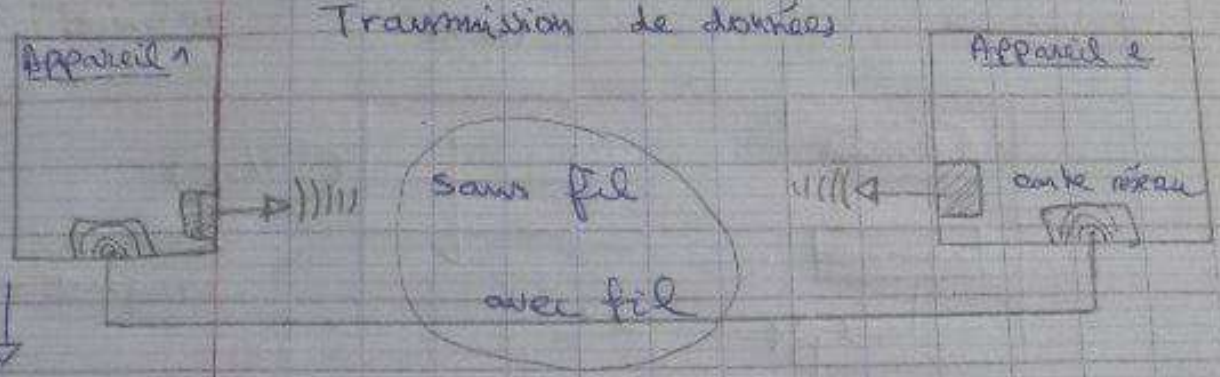
13/12/2019

Introduction :



codage des données

→ avec fil → 3 supports de transmission
- Paire torsadée.
- câble coaxial
- câble à fibre optique.

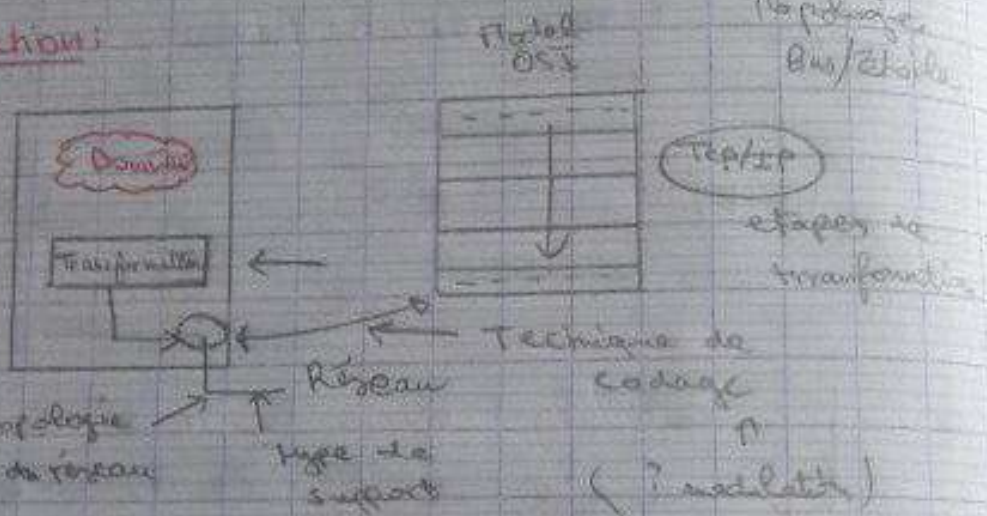
Bande de Base (avec fil)

Modulation (sans fil)

→ sans fil →
- Fréquence radio (wifi, ...)
- Rayon infrarouge (Télécommande

Chapitre 1 : Rappels sur les modèles de réseau OSI et TCP/IP

1- Introduction :



2- La transmission de données et les supports

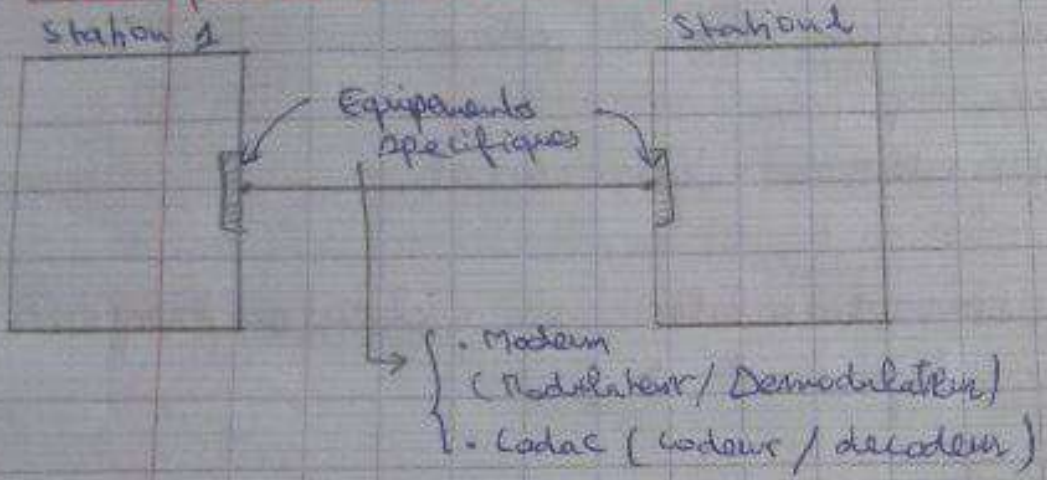
2.1- Les supports de transmission :

Trois familles de supports sont distinguées :

* Les supports métalliques (paire torsadée, câble coaxial) ⇒ transmission de donnée sous forme de courant électrique.
* Les supports non métalliques (fibre de verre, fibre de plastique) ⇒ transmission de donnée sous forme de lumière

* Les supports Immatériels (Ondes électromagnétique)
⟹ transmission de donnée sous forme de champs magnétique (developpé dans le chap 3)

2.2 Techniques de transmission :



L'equipement spécifique assure la fabrication des signaux en emission et la récuperation des données en reception.

• Techniques :

A) Transmission en Bandes de Base

+ Distance : < 1Km
+ support : paire torsadé, cable coaxial ou fibre optique.

0 ou 1
numérique

- Techniques de codage NRZ, NRZI, manchester, manchester différentiel, Miller

B) Transmission par Modulation :
+ Distance : ≥ 1 km ou plus
- L'existence d'un signal porteur
- La fibre optique
- Paire torsadée ou cable coaxial.

- Techniques : Modulation en amplitude, fréquence, phase

C) Transmission sans fil : wifi, Bluetooth
- Distance : selon la puissance
- signal porteur : Onde électromagnétique.

Technique : Modulation / Demodulation et autre.

2.3 Les types de transmissions

une seule ligne

↳ transmission simplex (ex : PC → Imprimante)

↳ transmission half-Duplex (ex : PC ↔ clé USB)

Deux lignes } supports différents

Transmission Full Duplex
(ex PC PC)

3.) Le modèle OSI :

OSI : Open système Inter connexion
(Interconnexion des systèmes ouverts)

7	Application
6	présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	physique

} couches logicielles
on ajoute j'usqu'à la couche physique

} Couches matérielles

3-1) Equipements d'interconnexion :

- Répéteur :

- pont } NRZI } Manchester

Ex [

- Routeur

- Passerelle : elle utilise toutes les couches (à partir des données on reconstitue le trame de 0)

3. c) Les méthodes d'accès au médium :

Trois méthodes essentielles peuvent être distinguées
+ Maître / esclave
+ Anneau à jeton [Token Ring]
+ Accès Aléatoire (CSMA / CD)

4- les protocoles TCP et IP:

Modèle OSI:

7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison
1	Physique

Modèle TCP/IP

Application
TCP
IP
Liaison
physique

TCP → Transmission fiable

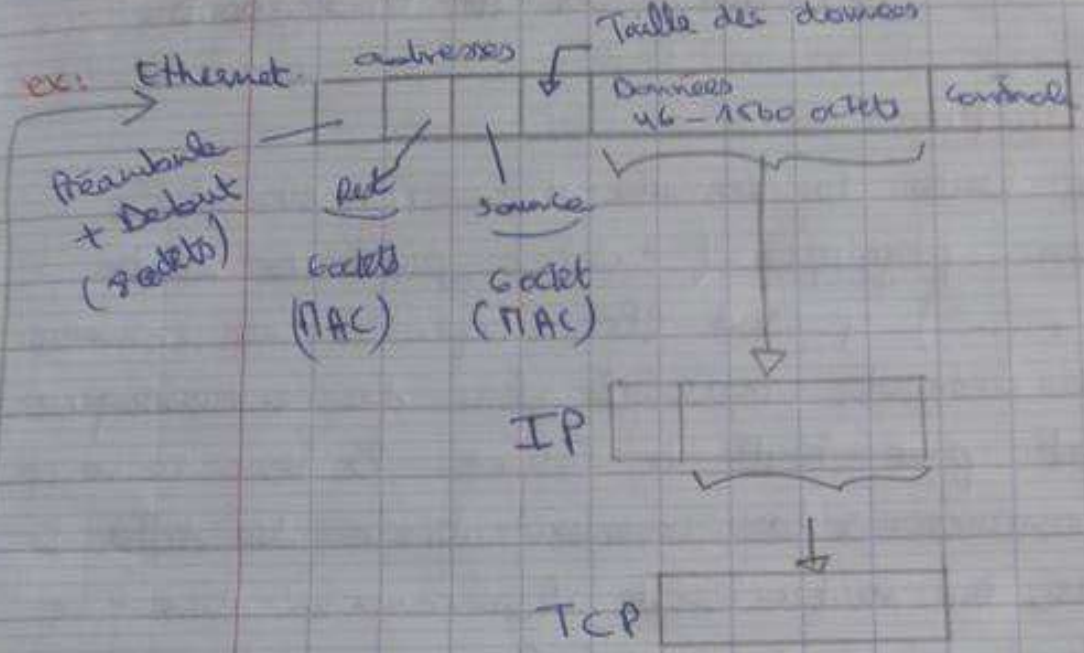
IP → Technique d'adressage

ex Ethernet

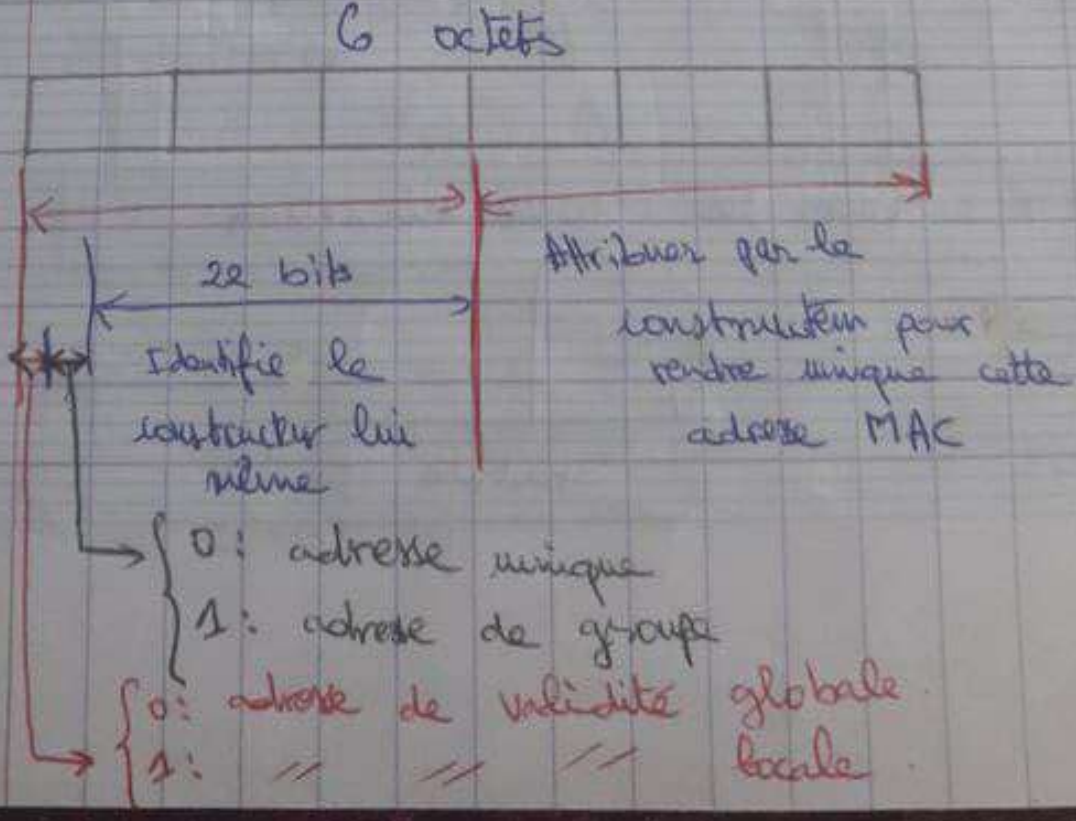
Liaison : CSMA/CD

physique : codage Connecteur

- Trame TCP et IP → (TP)



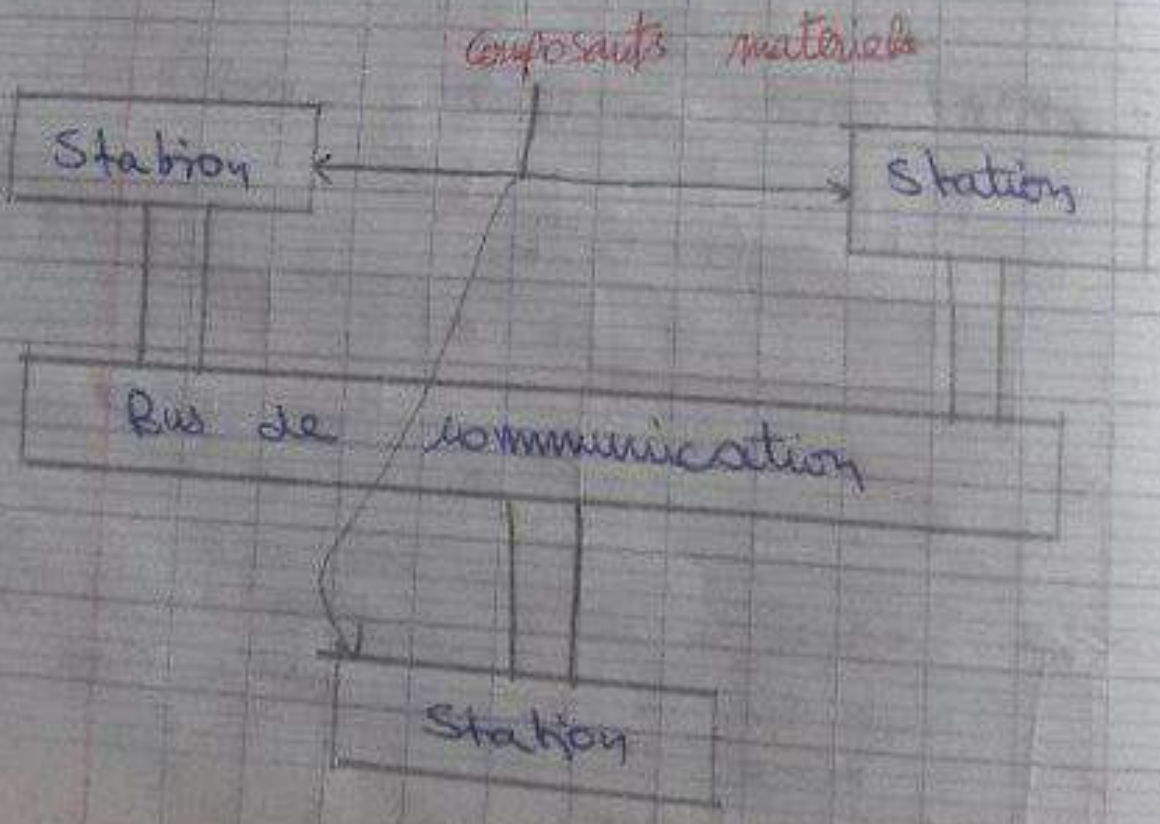
Adresse MAC: (Media Access control)



Chapitre 2: Bus de communication traditionnels et Emergeants.

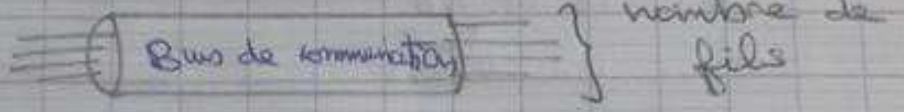
1- Introduction:

On appelle bus de communication un ensemble de liaison physique (cables, pistes de circuits imprimés, ...) pouvant être exploités en commun par plusieurs éléments materiels afin de communiquer. Les Bus ont pour but de réduire le nbre de voies (filés) nécessaires à la communication des différents composants, en mutualisant les communications sur une seule voie de données.



2- Caractéristiques d'un bus de communication

a. Le volume d'informations transmises simultanément



Le volume exprimé en bit correspond au nombre de lignes physiques (fils) sur lesquels les données sont envoyées de manière simultanée.
On parle également de longueur de bus.

b. La vitesse du bus de communication :
Se définie également par sa fréquence (Hz).
Elle correspond au nombre de paquets de données envoyées ou reçues par seconde.

c. Le débit maximal du Bus (taux de transfert maximal).
C'est la quantité de données qu'il peut transporter par unité de temps (seconde), en multipliant sa longueur par sa fréquence.

ex : longueur = 16 fils = 16 bits
- Fréquence = 133 MHz

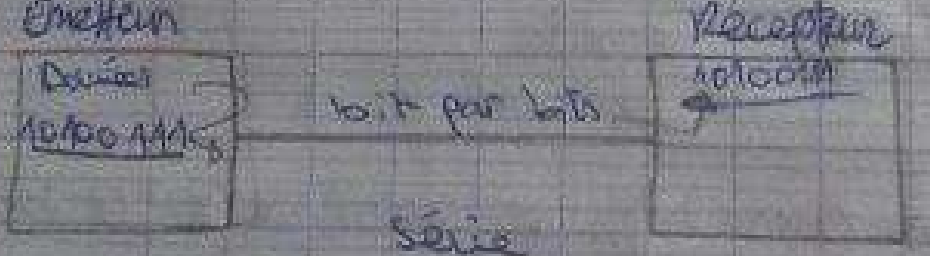
Débit = 16 · 133 M (bit . Hz)
= 2 . 133 M.O/s
↳ bauds

= 2 66 M O/s = 2,66 M bauds = 266 x 8 M bits

= 2133 M o/s
bits

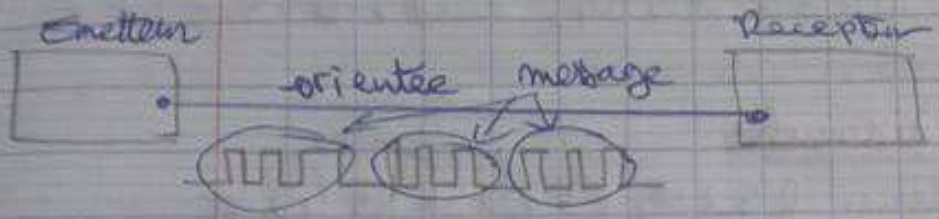
3. Classification des bus de communication

3.1. Classification selon la nature de la liaison



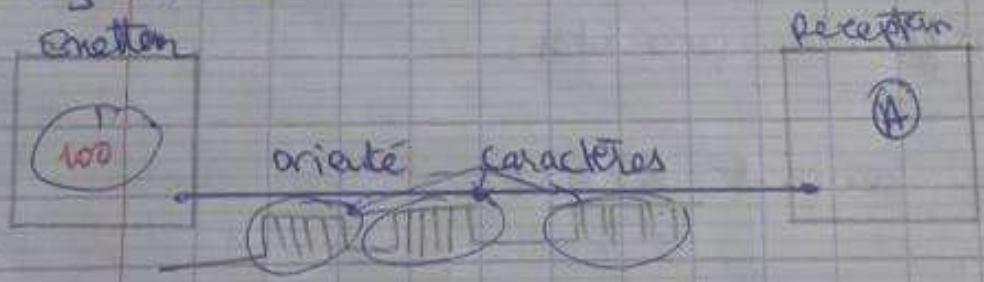
3.2. Classification selon leur cadencement.

- Bus synchrone :



même fréquence d'horloge

- bus asynchrone



fréquence d'horloge différentes

3.3 Classification selon le type de périphérique connecté :

Suivant les équipements connectés au bus de communication

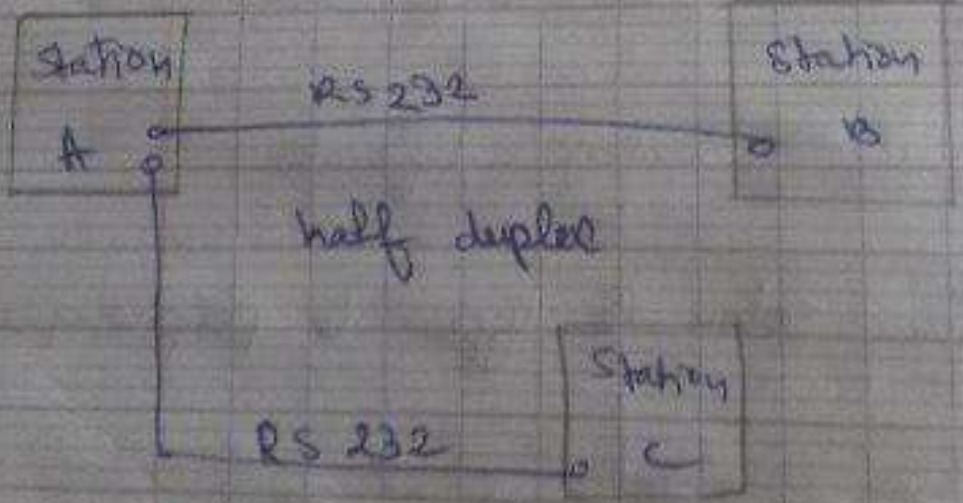
On distingue les bus traditionnels (RS232, RS422, RS485, Ethernet 10/100, I2C, SPI, Centronic, IEEE488, ...) et des bus emergents (USB, Giga Ethernet, IEEE 1394, card bus, SCSI, ...)

4. Les bus traditionnels:

4.1. Les bus séries RS232, RS422 et RS485

Les bus RS232, RS422 et RS485 sont des bus série asynchrone utilisé de manière générale en pilotage des procédés.

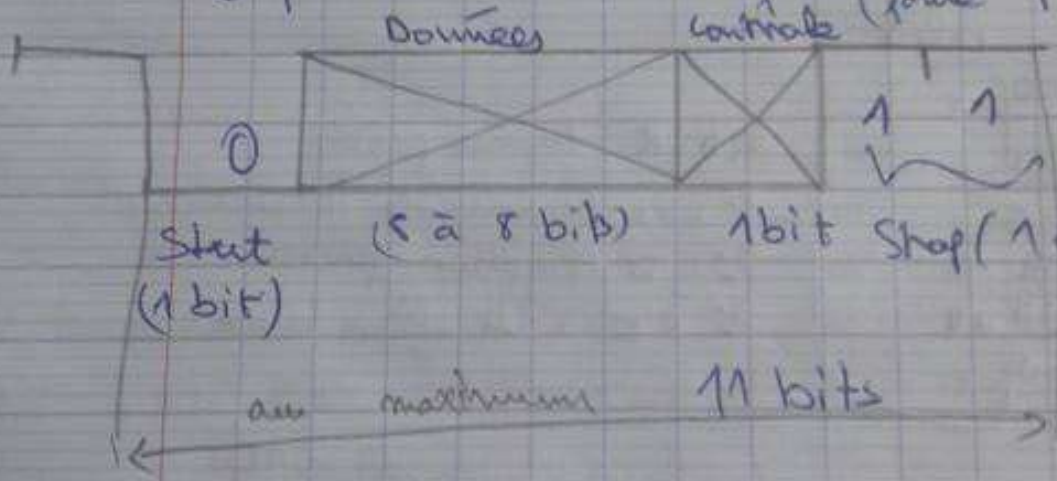
a. Le bus monopoint RS232:



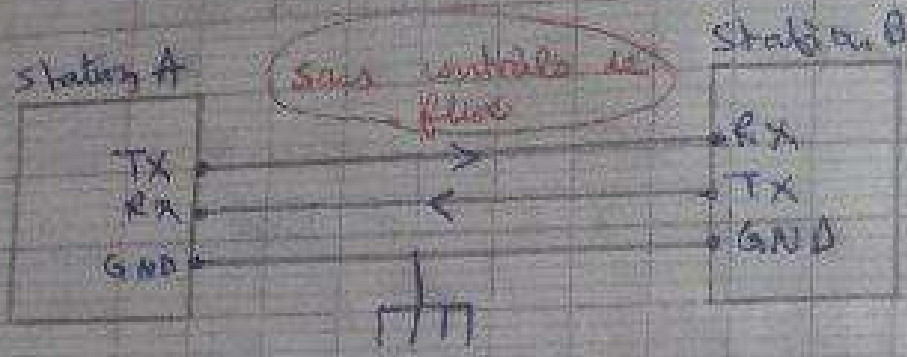
- Distance 15m au maximum.
- Débit théorique : 300 → 19 200 bauds.
- Signal électrique : tension.
  bit = "0" → +3 à +25 volt
  bit = "1" → -3 à -25 volts

Généralement Tension : -15 à +15 volt.

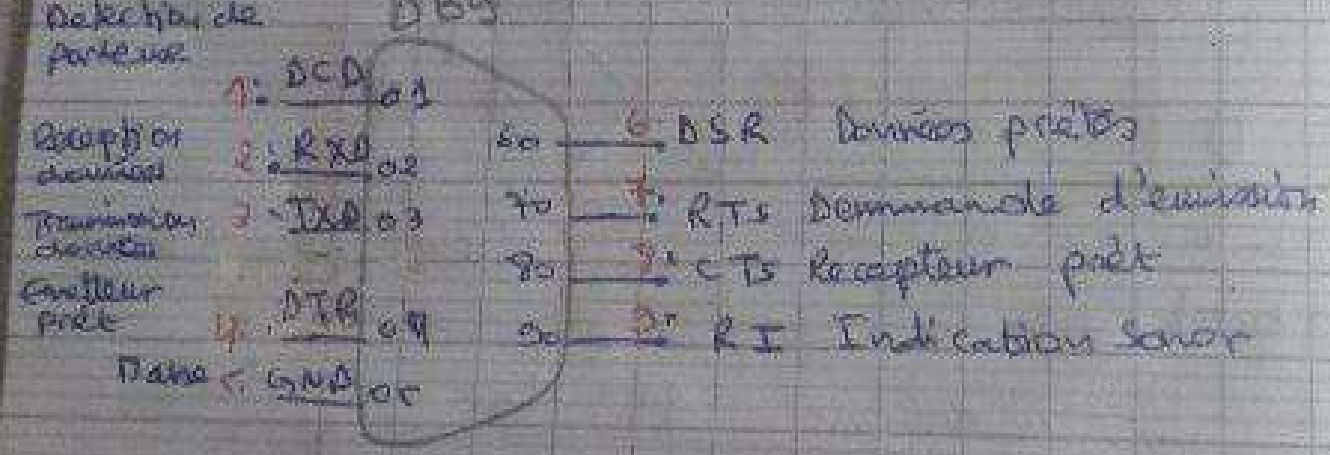
- Trame logique



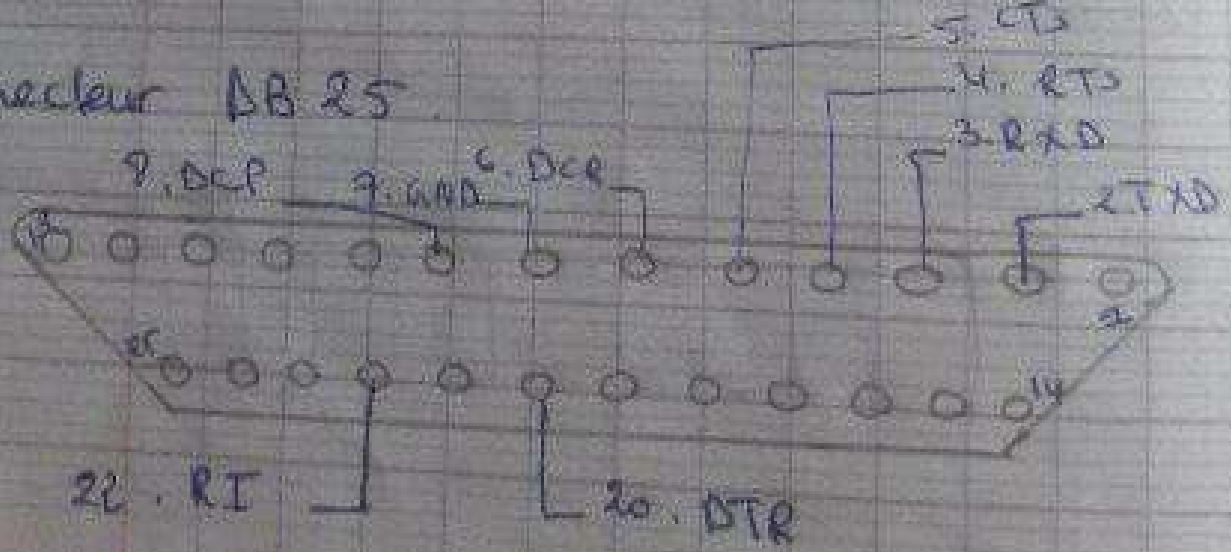
- les connexions du port série standard.



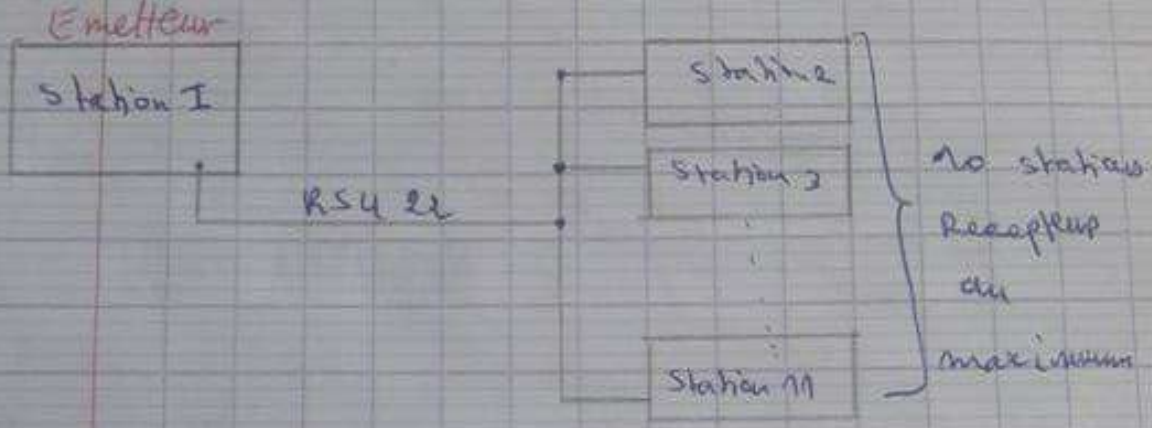
- Connecteur DB9



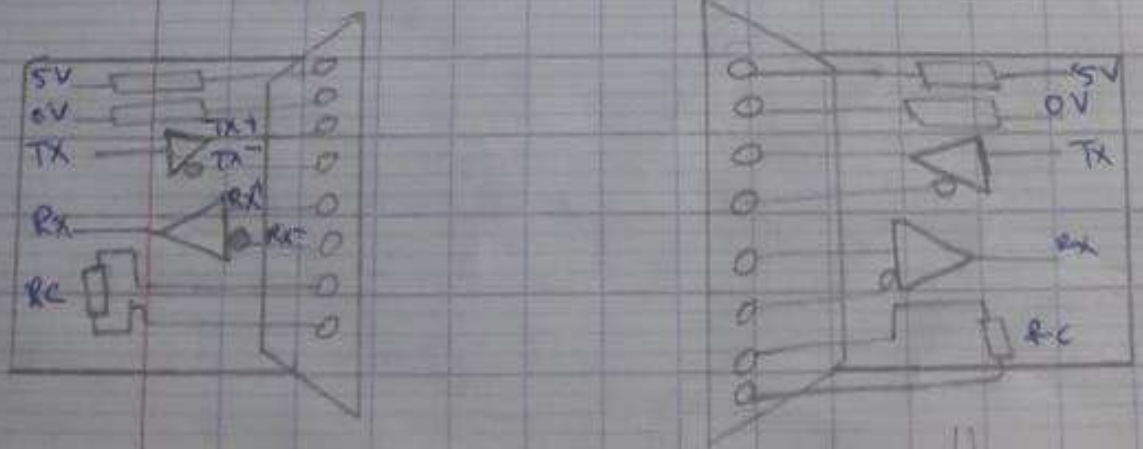
- Connecteur DB 25



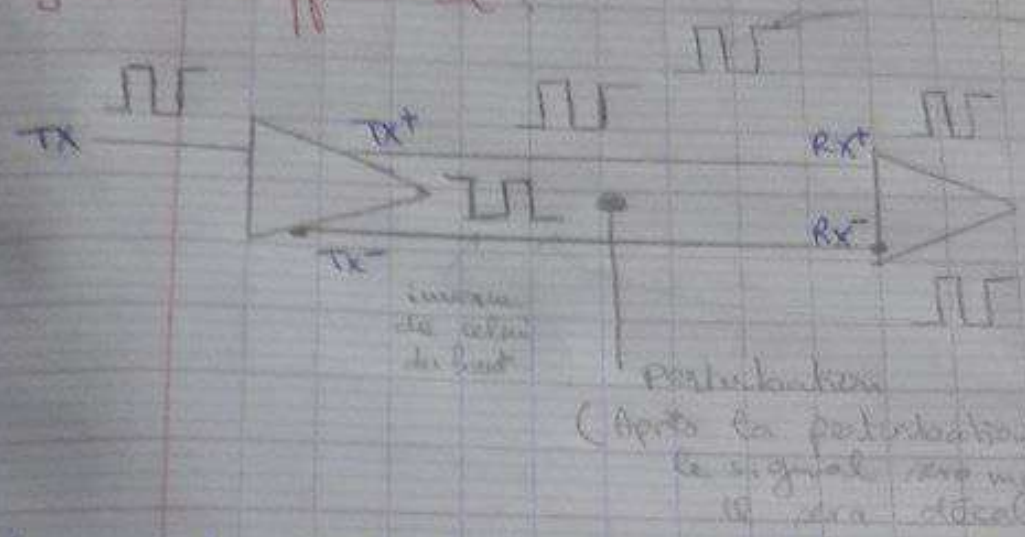
b. le bus RS 422 : (unidirectionnel)



- Un emetteur
- 10 Recepteurs au max
- Distance maximale : 1200 m
- Vitesse maximale : 100 Kb/s
- Transmission differentielle sur 5 fils (Tx+, Tx⁻, Rx+, Rx⁻, GND)
- Schéma de raccordement.

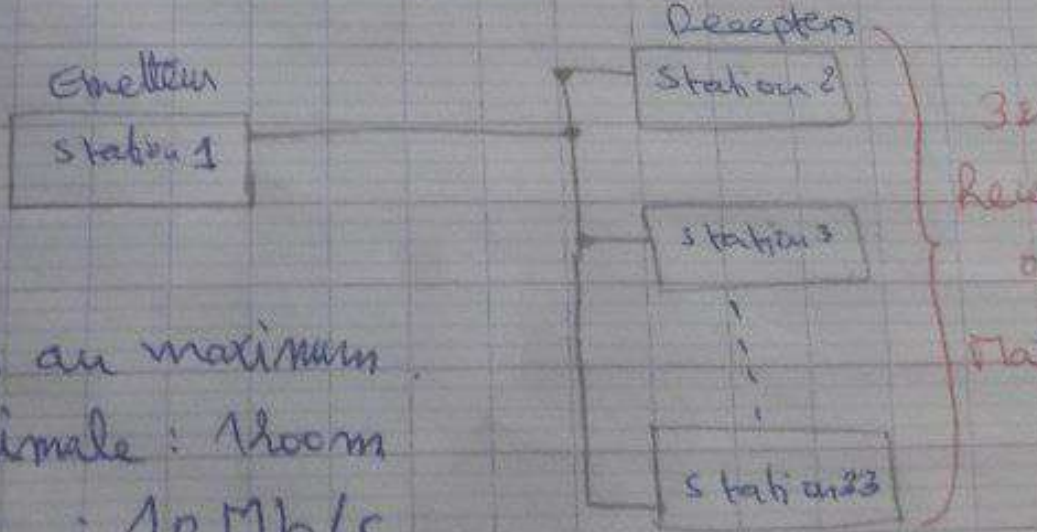


- Signal différentiel :



L'effet de la perturbation s'annule après la sommation des deux signaux Rx+ et Rx- le signal RX sera le double du signal TX

c- Le bus RS 485 (Bidirectionnel)



- Un Emetteur
- 32 recepteurs au maximum
- Distance maximale : 1200m
- vitesse " : 10 Mb/s

4.2 . le bus I2C : (Interface Integrated circuit)

- C'est bus série, synchrone, bidirectionnel, et. half - duplex.
Il est dédié aux circuits intégrés.

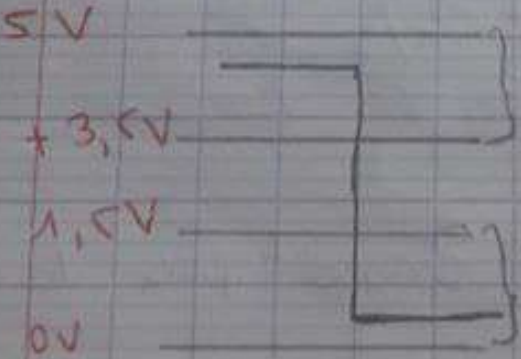
- Raccordement sur 3 fils :

SCL	— Horloge fournie par le maître
SDA	— Données dans les deux sens.
GND	— Masse.

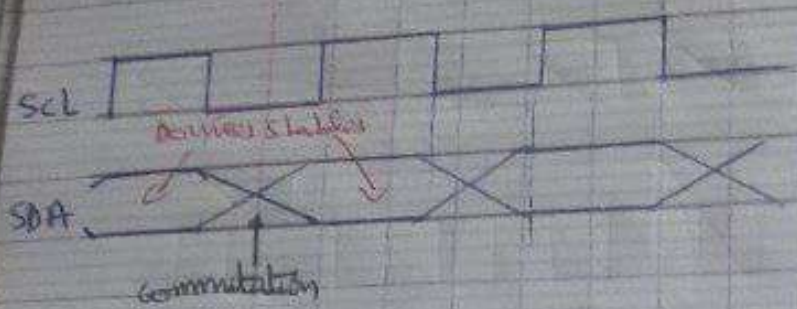
- La fréquence maximale est de 100kHz, soit 100kb/s
- Amplitude des signaux.

Niveau haut $\geq 0,7 \times V_{cc}$ ($V_{cc} \simeq 5$ volt)

Niveau bas $\leq 0,3 \times V_{cc}$

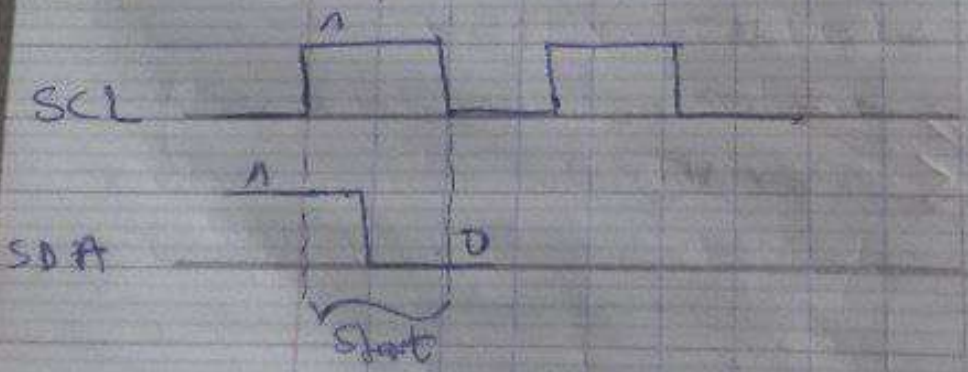


- Fonctionnement maître / esclave
- La trame de données I²C

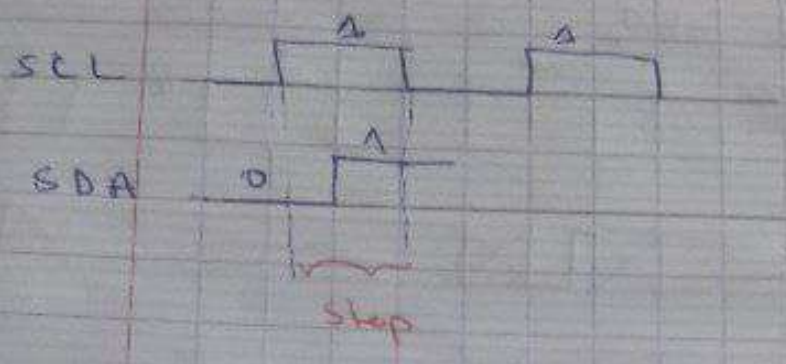


- les données sur SDA ne changement que quand SCL est bas : Elle sont stables pour SCL est haut.

* Start : Donnée sur SDA change (passe de 1 à 0) quand SCL = 1



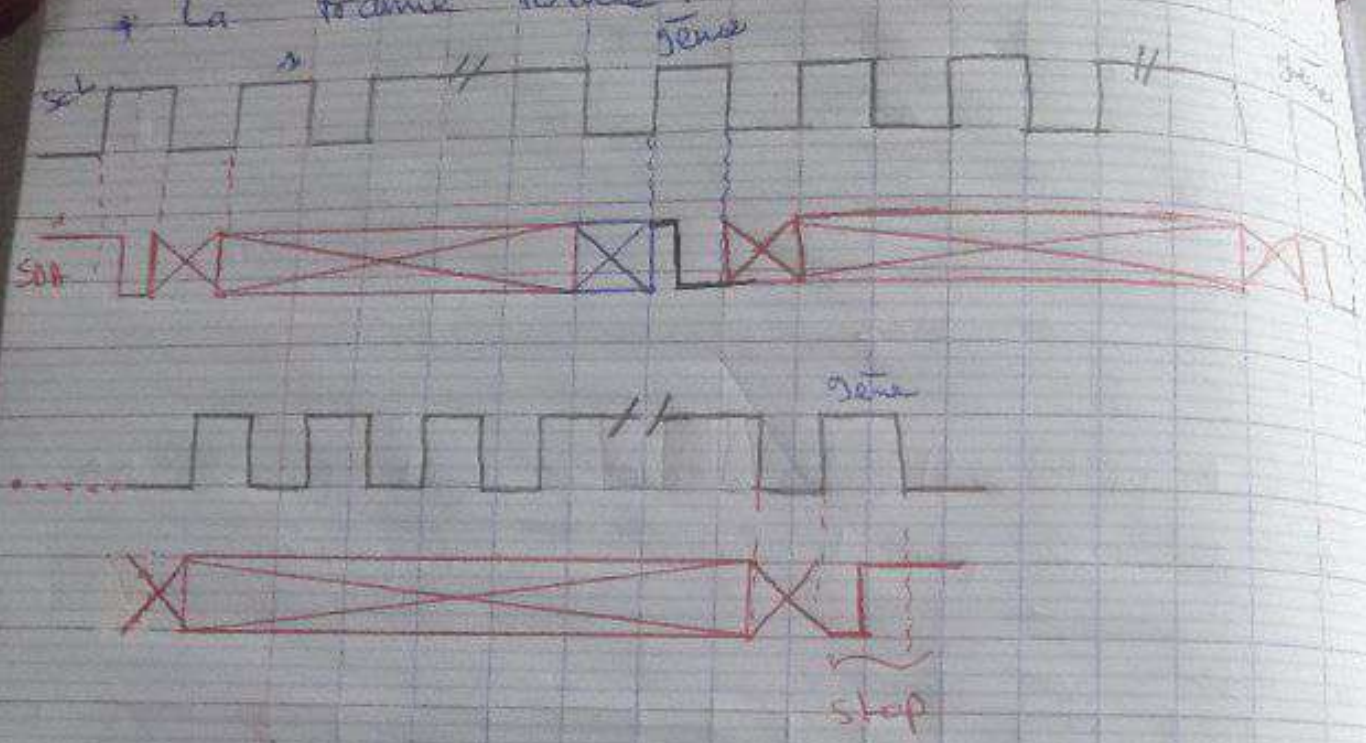
* Stop : Donnée sur SDA change (passe de 0 à 1) quand SCL = 1



- ACK (Acquittement) : le récepteur fait passer SDA de "1" à "0" pendant la 9ième impulsion de SCL.

- le premier octet :

* La trame totale :



4.3 Le Bus Ethernet 10/100.

Le Bus Ethernet est mis au point dans les années 80 par XEROX, INTEL, DEC il permet l'interconnexion de matériel divers avec de grandes facilités d'extension.

a- Bus Ethernet à 10 Mb/s :

- Norme IEEE 802.3 10 base 5 et 10 base 2.

10 base 5 → câble coaxial de longueur maximale 500m
10 Mb/s
technique de codage en bande de base

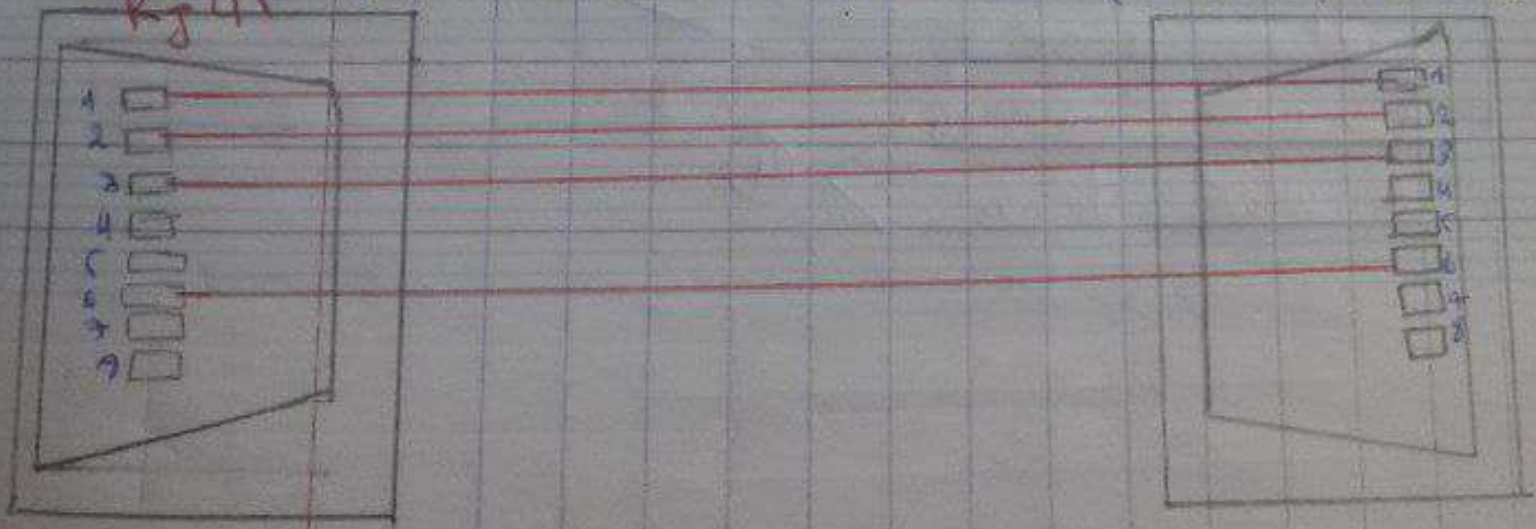
10 base 2 → câble coaxial longueur (185m)
10 Mb/s
bande de base

- Norme IEEE 802.3 10 base T

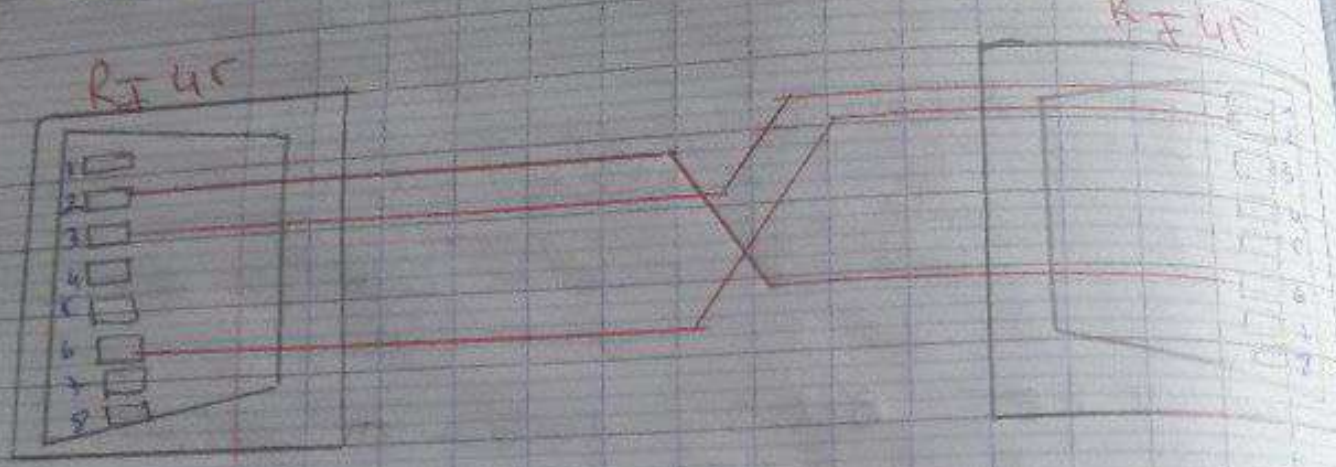
10 base T → Paire torsadée (2 paire) longueur maximale 100m
10 Mb/s
bande de base

- câble à 4 fils (2 pairs torsadés) avec des connecteurs RJ45.

* **câble droit** : Il permet la connexion d'une station (PC) à un concentrateur (switch, Routeur, ...)



- Cable croisé : Il permet la connexion de deux stations entre elles ou de deux concentrateurs entre eux.



- Normalisation des couleurs sur un câble Ethernet torsadé.

1. TX + Blanc vert
2. TX - Vert
3. RX - Blanc Orange
4. Non utilisé Bleu
5. Non utilisé Blanc Bleu
6. RX + Orange
7. Non utilisé Blanc Marron
8. Non utilisé Marron

(1) (2) (3) (4)

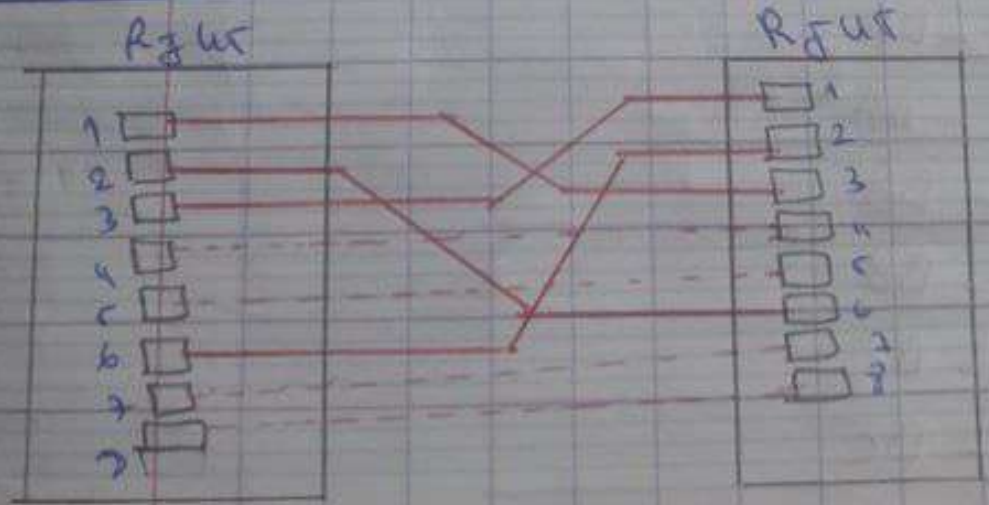
b_ Fast Ethernet à 100 Mb/s

- Norme IEEE 802.3u 100 base TX

100 → 100 Mb/s
base → bande de base
TX → 2 paires torsadées (4 paires) | longueur 100 m)

- cable droit :

- cable croisé :



~~Bus emergents~~

5- Les Bus emergents :

5-1 le Bus Giga Ethernet à 1 gb/s et plus

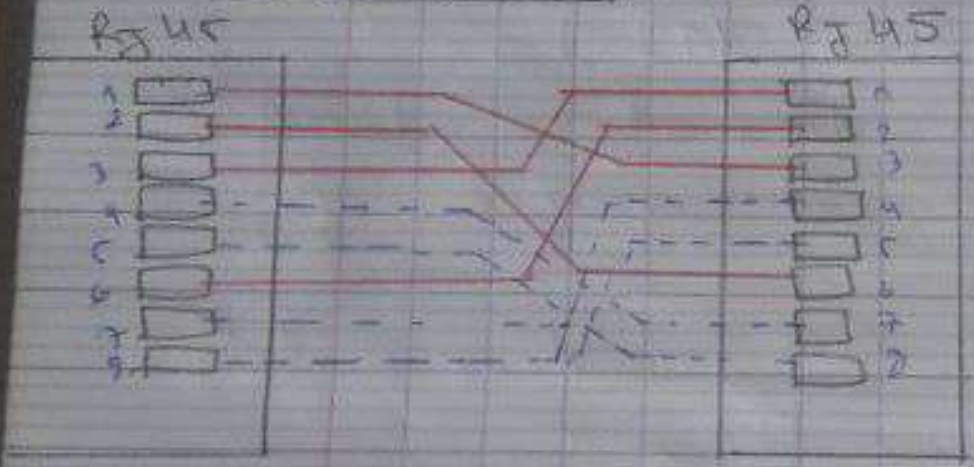
- Norme IEEE 702. 3ab 1000 baseT

1000 base T

1000 Mb/s bande de base

la paire torsadée

- câble croisé :



1. + BI - DA
2. - BI - DA
3. + BI - DB
4. - BI - DB
5. + BI - DC
6. - BI - DC
7. + BI - DD
8. - BI - DD

DA, DB, DC et DD sont les données.
BI : Bidirectionnel

5.2 le bus USB.

U.S.B. Universal Serial Bus.

à la base, le bus U.S.B est un Bus série, asynchrone et Half Duplex. Il permet une connexion à chaud (appareil en état de fonctionnement).

Il existe 2 différents ensembles de versions de Bus USB :

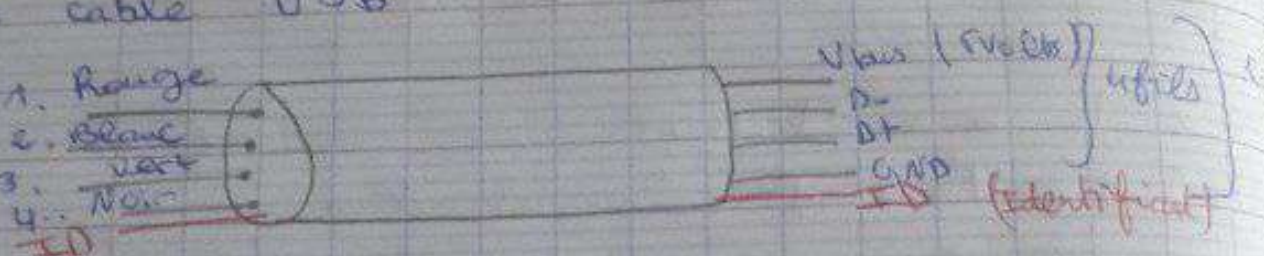
- Le premier ensemble englobe les versions 2.0 et antérieures.
- Le deuxième ensemble englobe les versions 3.0 et postérieures.

antérieurs

1.0 1.1 1.2 2.0 3.0 3.1 3.2 actuellement

a - les versions 2.0 et antérieures :

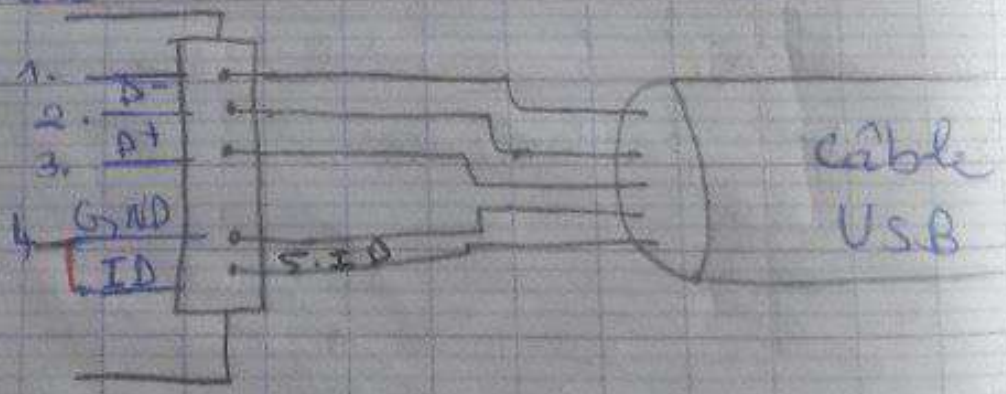
- le cable USB



4 fils pour les connecteurs standards
5 fils pour // // de type mini ou Micro

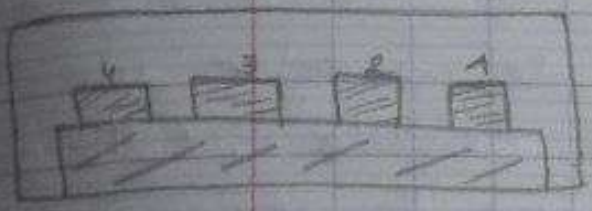
le fil N°5 (ID) permet d'identifier l'equipement maître : il est relié à la masse du côté de l'équipement maître.

Equipements maître

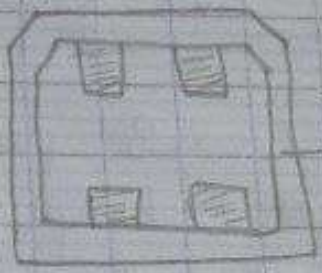


- Les connecteurs :

Type A



Type B



- La vitesse de transmission

USB 1.0 1,5 Mb/s

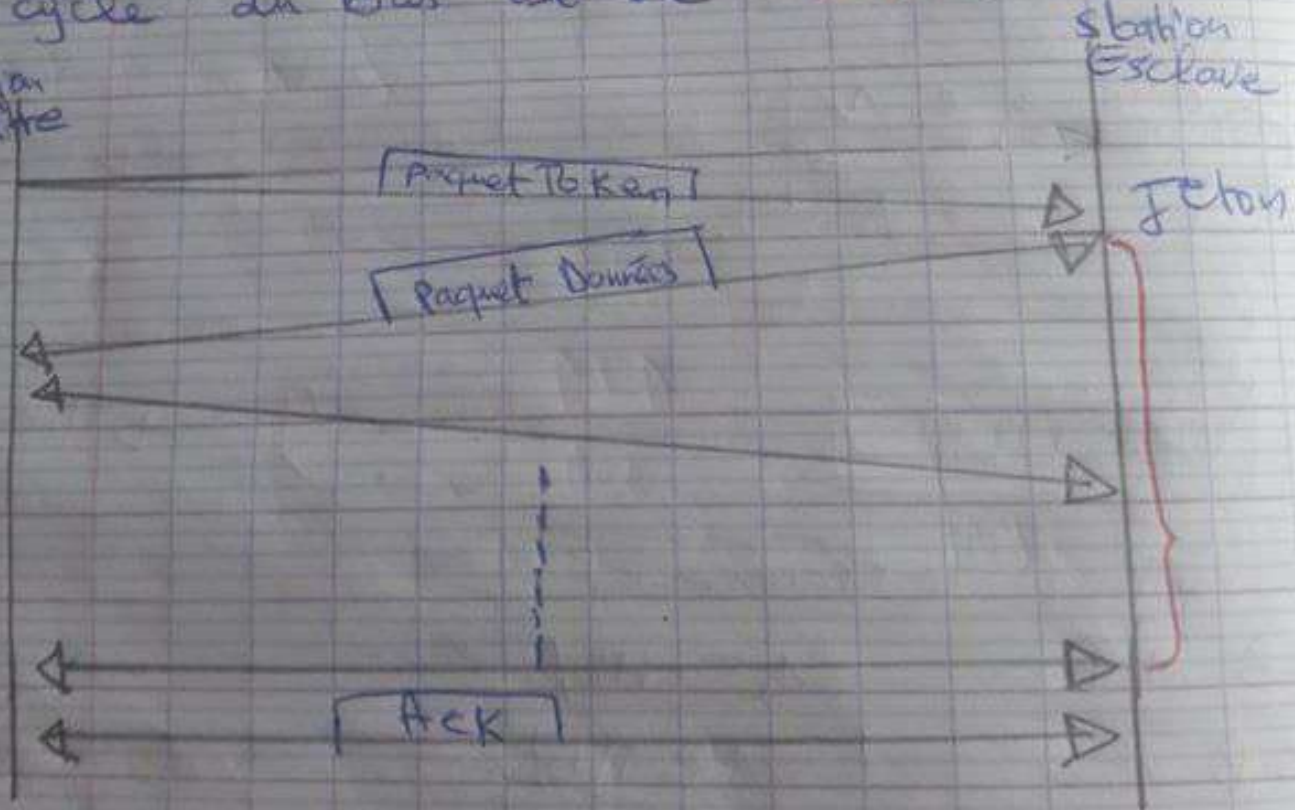
USB 1.2 12 Mb/s

USB 2.0 480 Mb/s

- Technique de codage des données : NRZI
- Transfert des données : Techniques de l'anneau à Jeton (Token Ring).

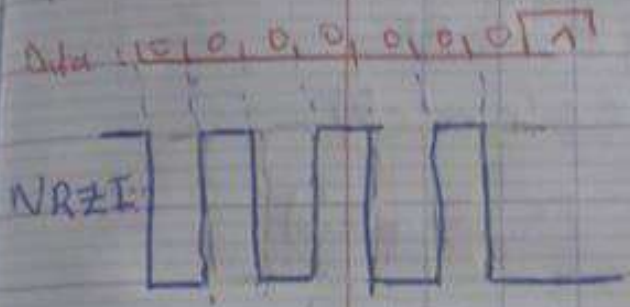
* Principe de fonctionnement :

Un Bus U.S.B permet de connecter un nbre limité d'équipements esclave. Cette limite vient du fait que le temps du cycle du Bus est de 1 ms.



- Structure des paquets
  - Token
  - Data
  - Ack

8 bits	Paquet			2 bits
Synchronisation	Paquet ID	Paquet Information spécifique	CRC	EOP

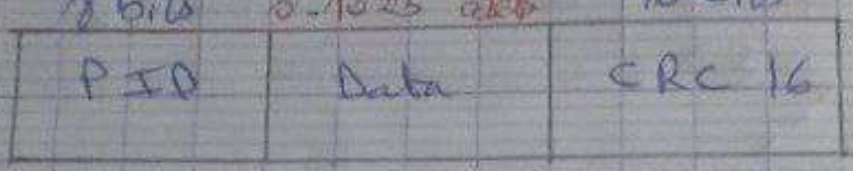


- Format des paquets :
  - Paquet Token

8 bits	7 bits	4 bits	5 bits
PID	ADDR	ENDP	CRC5

1001 IN : Données de l'esclave vers le maître
0001 OUT : // du Maître vers l'esclave.
1101 SETUP : Installation de l'esclave (configuration)

- Paquet Data :



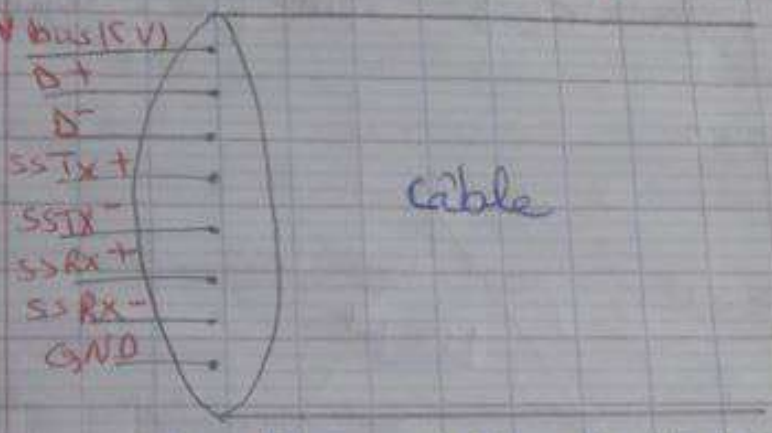
(0011) Data 0 : Faible vitesse : (8 octets).
(1011) Data 1 : Pleine Vitesse (64 octets)
(0111) Data 2 : } grandes vitesse (1023 octets)
(1111) Data A : }

- Paquet ACK

Validation ← ACK : 0010
Refus de données ← NACK : 1010
STALL : 1110 → Stop
NYET : 0110 → Pas de réponse

b- les versions 3.0 et postérieurs

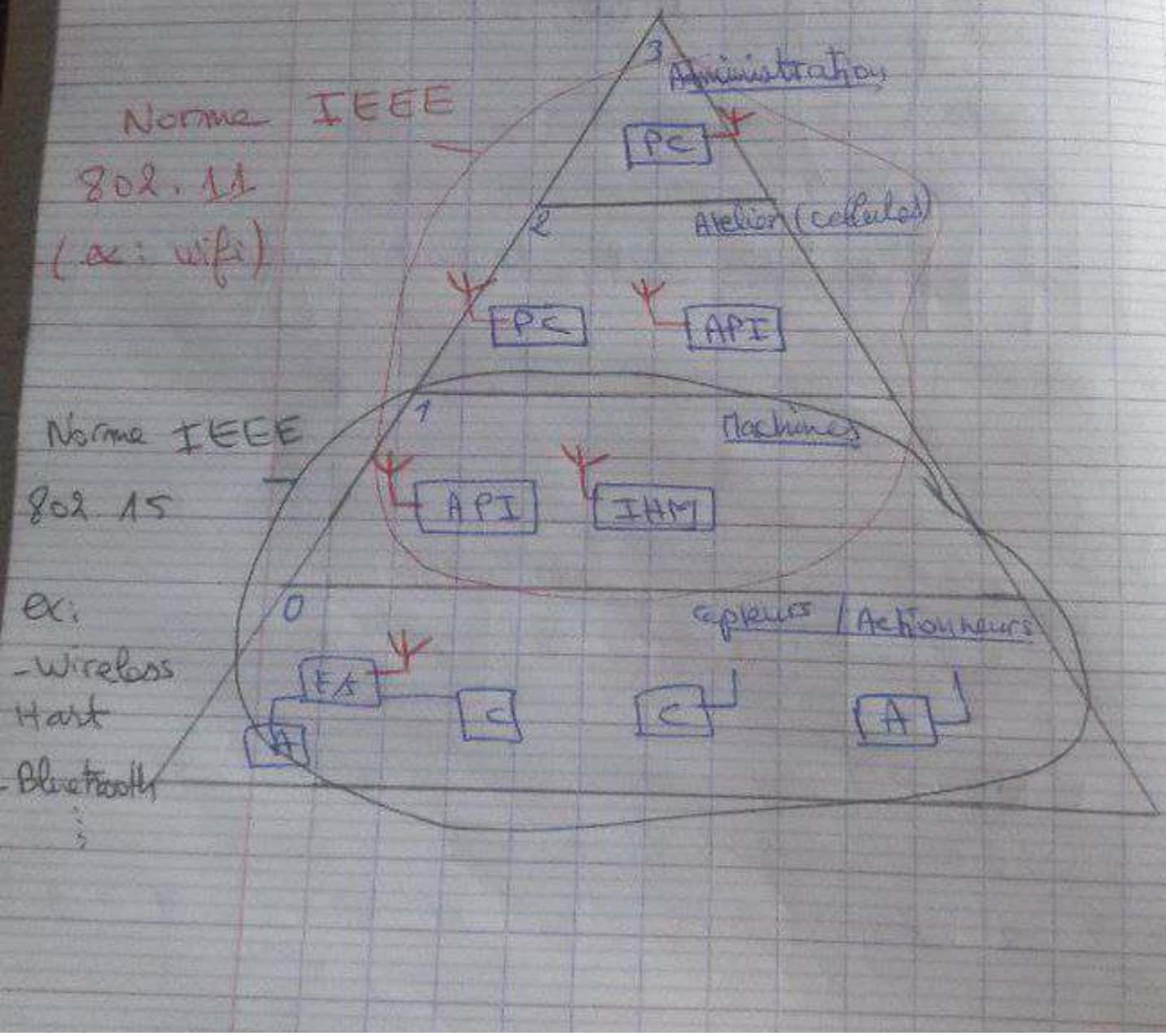
- le cable USB (SS : Super Speed)



Le Bus USB devient Full-Duplex

Chapitre 3: Protocoles de communication industrielle sans-fil - wireless HART

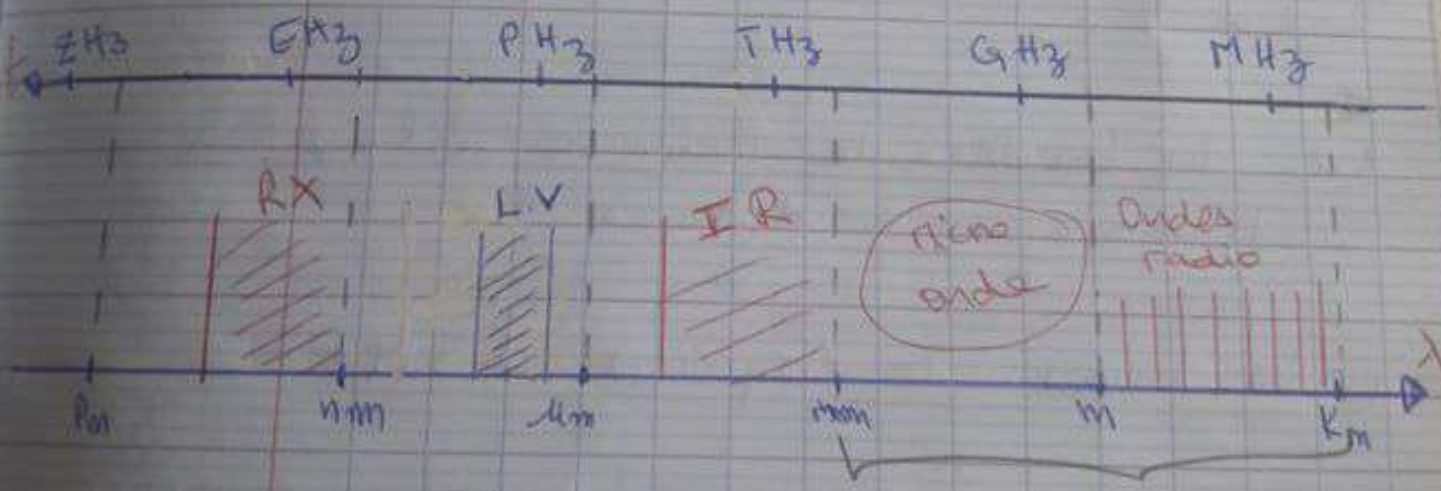
1. Introduction:



Après le succès de la téléphonie mobile, les technologies sans fil s'appliquent désormais aux réseaux locaux (WLAN : Wireless Local Area Network) aux réseaux personnels (WPAN : Wireless Personal Area Network) et aux réseaux capteurs (WSAN : Wireless Sensors Area Network).

2- Notions de bases:

2.1 Le spectre électromagnétique :



- Les domaines utilisés en transmission sans fil:

Domaine	Fréquences	Longueurs d'ondes
Infrarouge	3THz - 400THz	750 nm - 0,1 mm
Micro-Ondes	300MHz - 300GHz Wifi, Bluetooth	1 mm - 1m
Ondes Radio	3Hz - 300MHz	1m - 100000 Km

2.2- les bandes de fréquences utilisées en transmission de données:

a- les bandes de fréquences ISM:

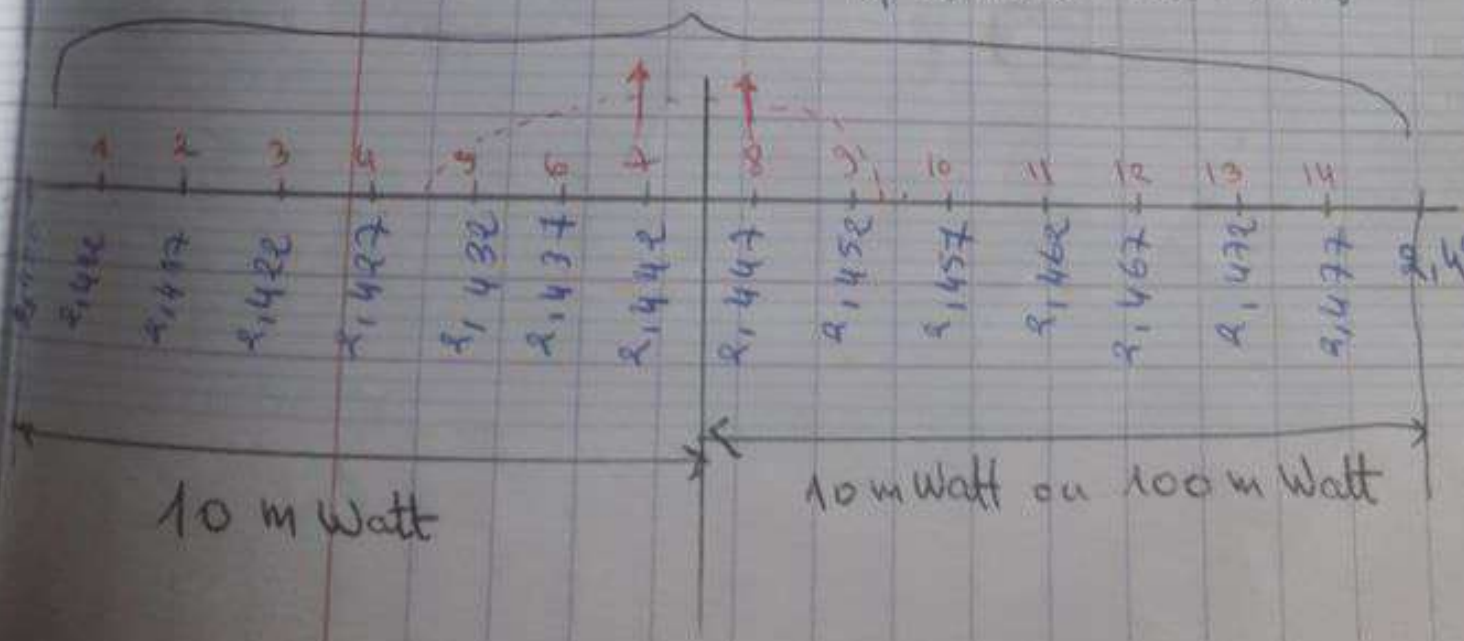
ISM: Industrielle, Scientifique et Médicale.

Les ISM sont utilisées, sans licence, pour des applications de télécommunication de faibles portées (centaines de mètres)

- les bandes basses 433 MHz et 868 MHz.

Exemples d'utilisation:
- Domotique (télécommande portail, ...)
- Véhicule (Télécommande voiture ...)

- Bande 2,4 GHz.

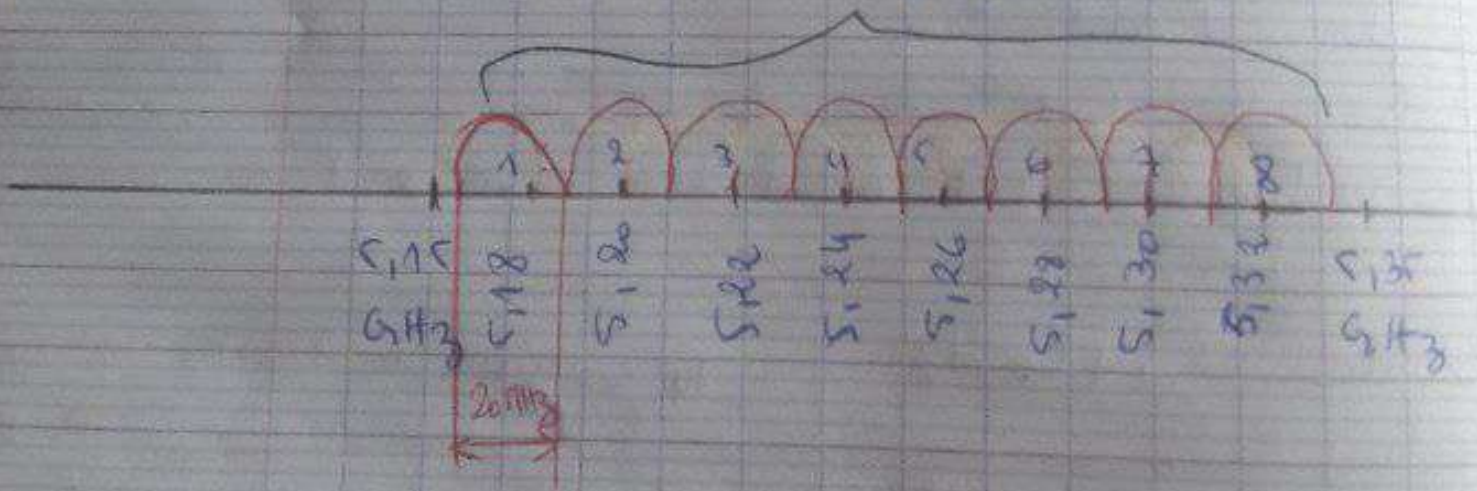


En pratique les séquences de fréquences utilisées sont : 1, 6, 11 ; 2, 7, 12 ; 3, 8, 13

b- La bande de fréquence U-NII :

U-NII : (Unlicenced - National Information ~~Institute~~ Infrastructure)
Informations nationale d'infrastructure sans licence.

- la bande de 5 GHz.

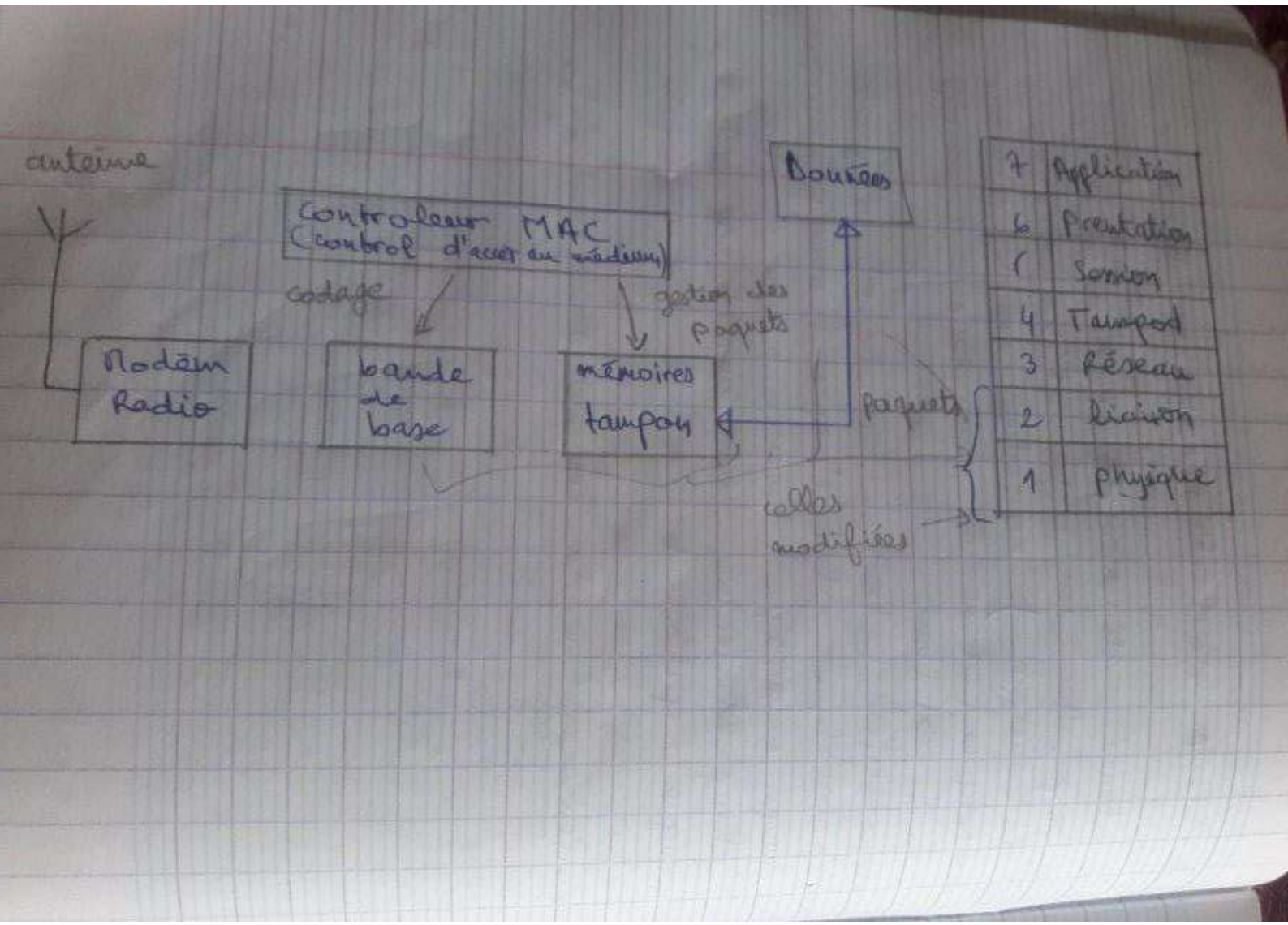


2-3. Principe de fonctionnement des antennes:

Une antenne radio électrique (formation et propagation des ondes électromagnétique à faible énergie) convertie des grandeurs électriques dans un conducteur ou une ligne existantes de transmission (tension ou courant) en grandeur électromagnétique dans l'espace (champs électriques et champs magnétique) inversement en réception le champs électrique est converti en signal électrique qui peut ensuite être amplifié.

2-4 - Principe de la communication sans fil:

↳

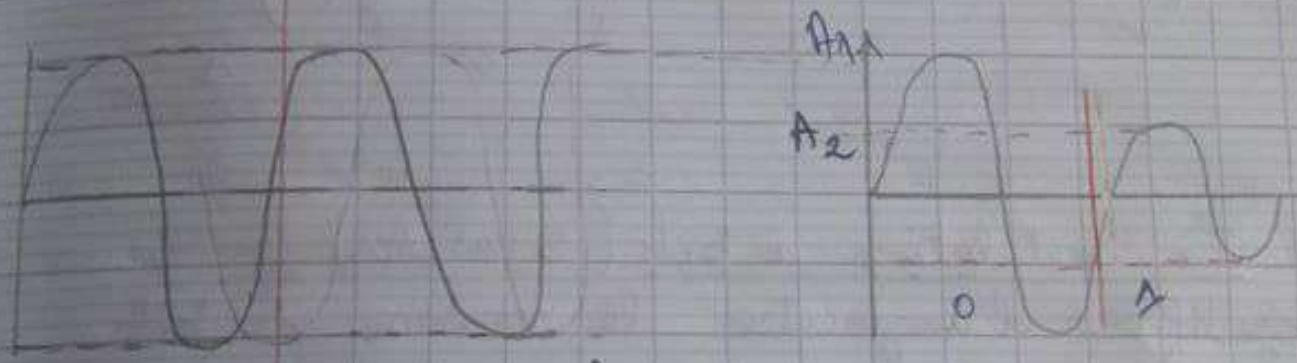

antenne
Contrôleur MAC
(control d'accès au médium)
codage
gestion des paquets
Modem Radio
bande de base
mémoires tampon
Données
paquets
collés modifiés
7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 liaison
1 physique

3_ Les modulations radio :

Les modulations fondamentales sont :

. Modulations d'amplitude ASK (Amplitude Shift Keying)

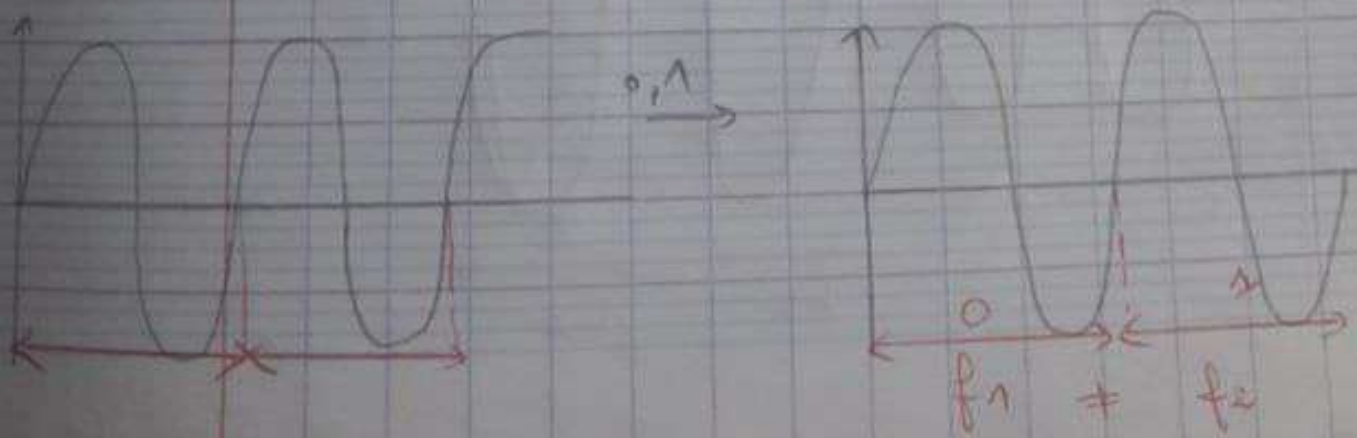
Codage pas d'amplitude :



porteuse du signal

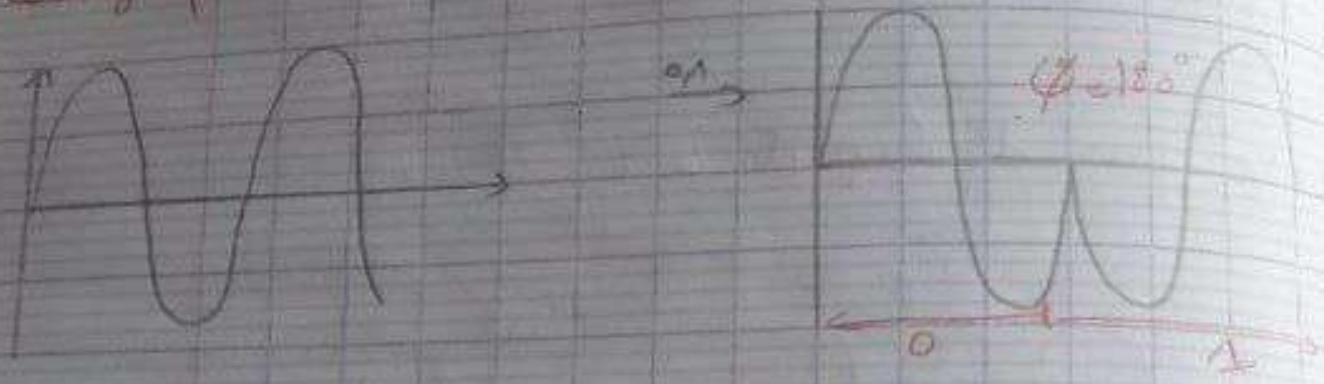
. Modulation de fréquence FSK (frequency shift Keying)

codage par décodage de fréquence :



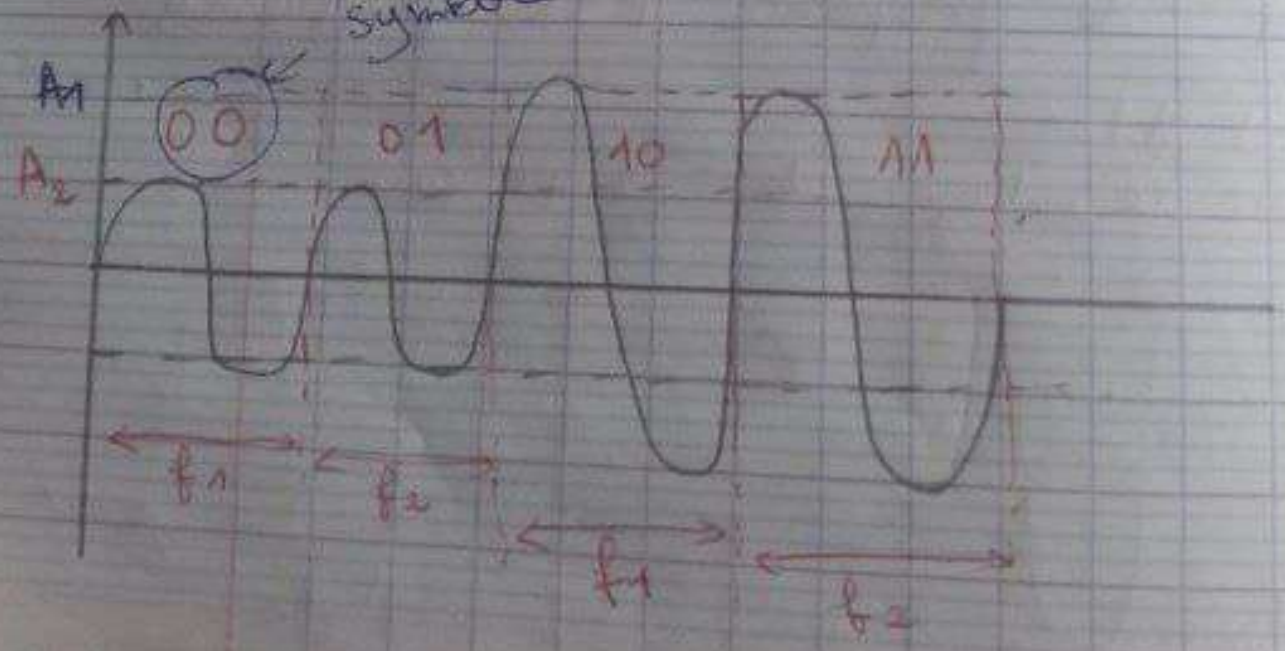
- Modulation de phase PSK (phase shift keying)

codage par décodage de phase:



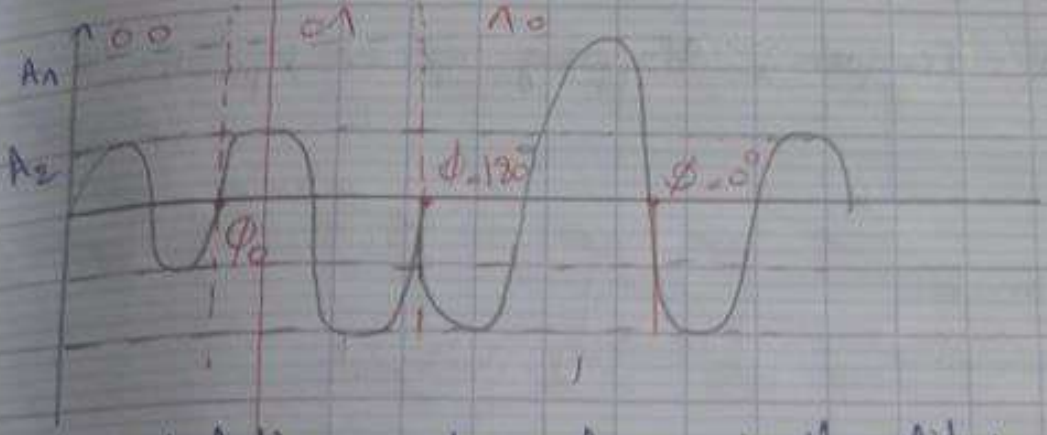
3_1 La modulation à bits (symboles)

L'objectif est d'augmenter le nombre de bits transmis par chaque période de la porteuse (signal) par exemple:



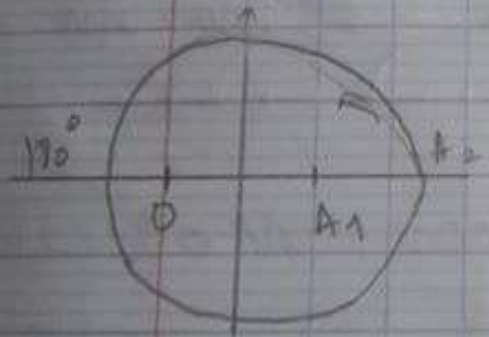
⇒

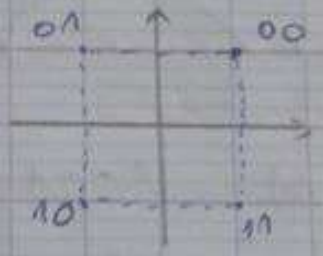
⇒ Modulation de fréquence et d'amplitude.



⇒ Modulation de phase et d'amplitude

3.2/ Combinaison avec quadratique: (ΦPSK)





2ΦPSK

4ΦPSK

8ΦPSK

3 bits

16ΦPSK

4 bits

64ΦPSK

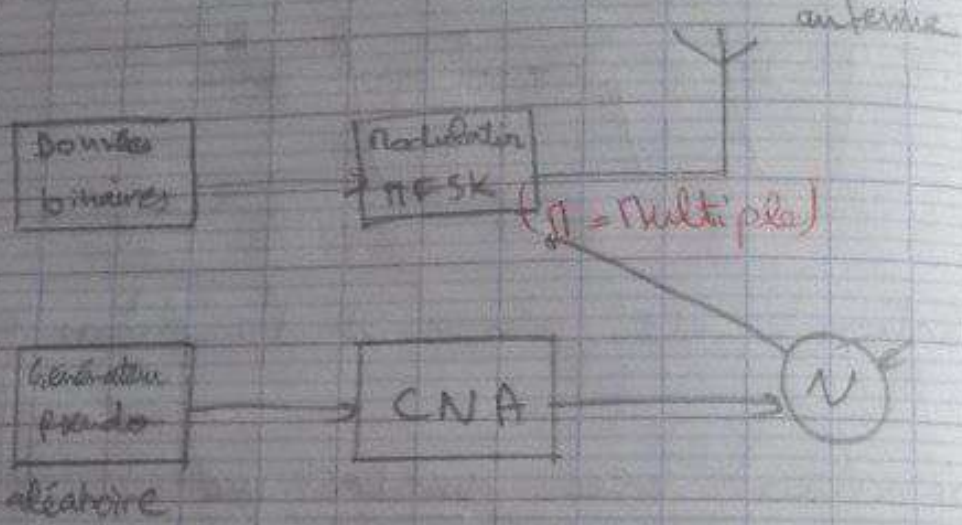
6 bits

128ΦPSK

3.2/ Application de la modulation à bits multiples :

a/ Le FHSS : Frequency Happing spread Spectrum

schéma :

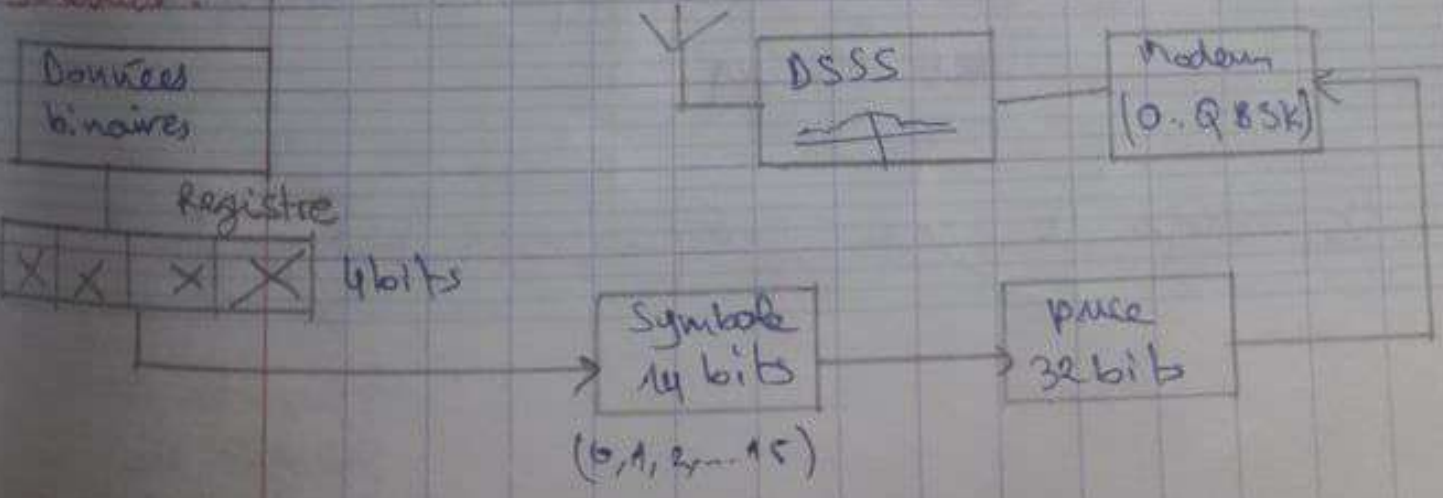


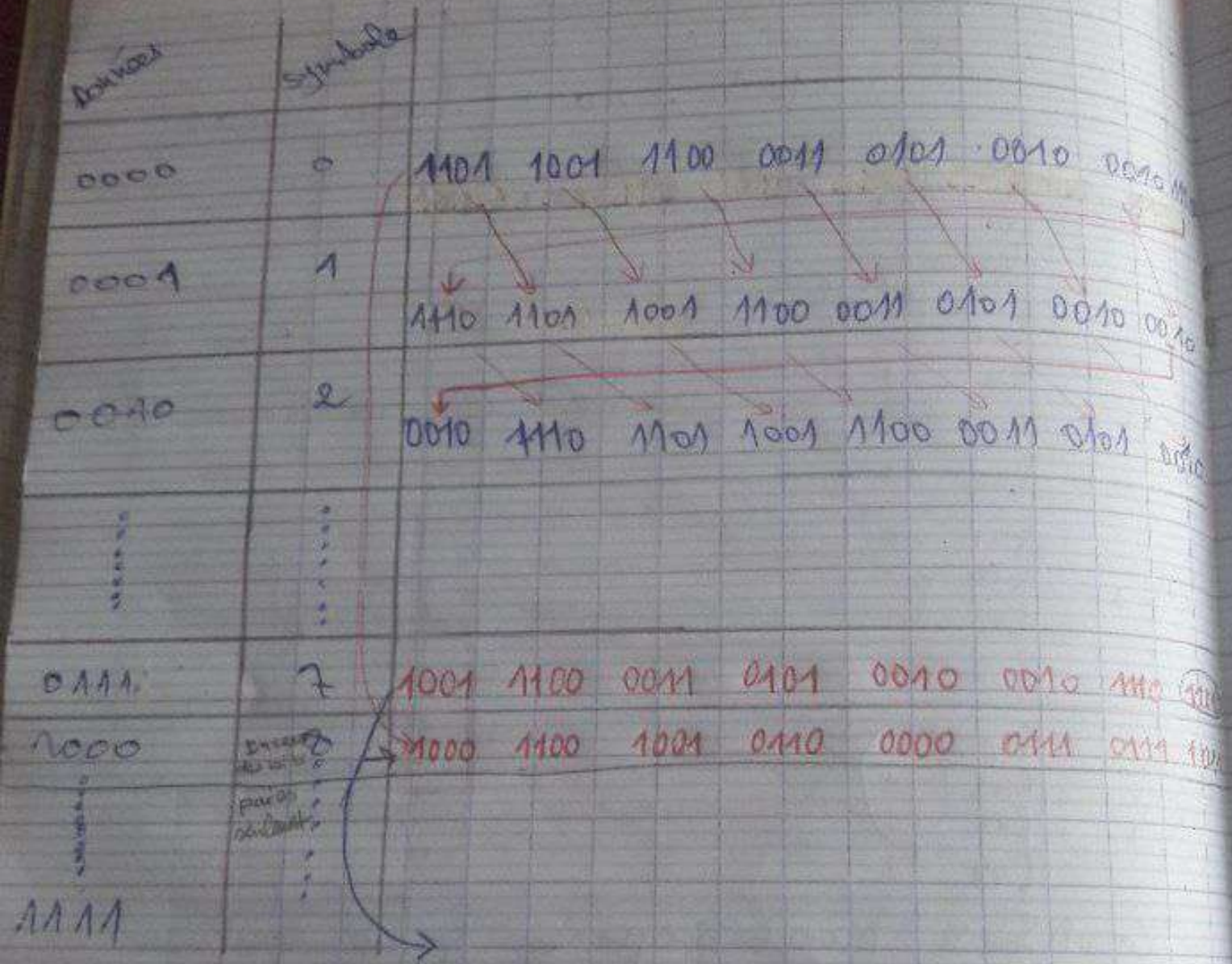
Données : 1011 1001 1000 1101

			1011	1001	1000	1101
00/F_{C1}	f_{11}	00				
	f_{12}	01				
	f_{13}	10				
	f_{14}	11				
01/F_{C2}	f_{21}	00				
	f_{22}	01				
	f_{23}	10				
	f_{24}	11				
10/F_{C3}	f_{31}	00				
	f_{32}	01				
	f_{33}	10				
	f_{34}	11				
11/F_{C4}	f_{41}	00				
	f_{42}	01				
	f_{43}	10				
	f_{44}	11				

b/ Le DSSS Direct sequence spread spectrum.
Elements du spectre par sequence direct.

schémas :





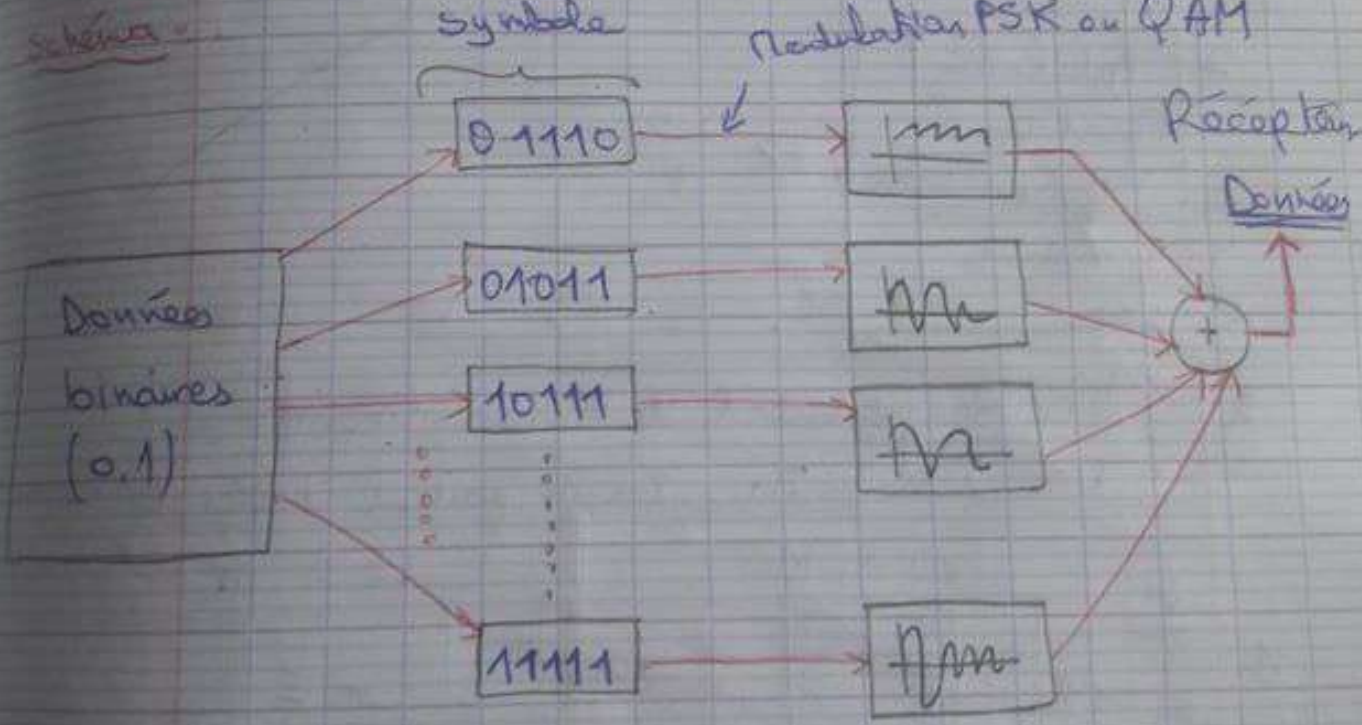
c- l'OFDM : Orthogonal Frequency Division Multiplacing

Multiplexage de sous fréquence orthogonales

↑
choisi de sorte à ne pas avoir de chevauchement

Pour la 2,4 GHz comme exemple.

Schéma :



Pour éviter le recouvrement (chevauchement) entre les sous porteuses (sous fréquences) le sys fonctionne suivant une choix de sous fréquences orthogonales.

4/ Les réseaux sans fil :

a.1/ Le model OSI et les réseaux sans fil :

7	Application
6	Présentation
5	session
4	Transport
3	Réseau

⇒ couche haute

2 — liaison : LLC 802, 2 control de liaison logique
MAC 802, 11/MAC 802, 15 control d'accès au support

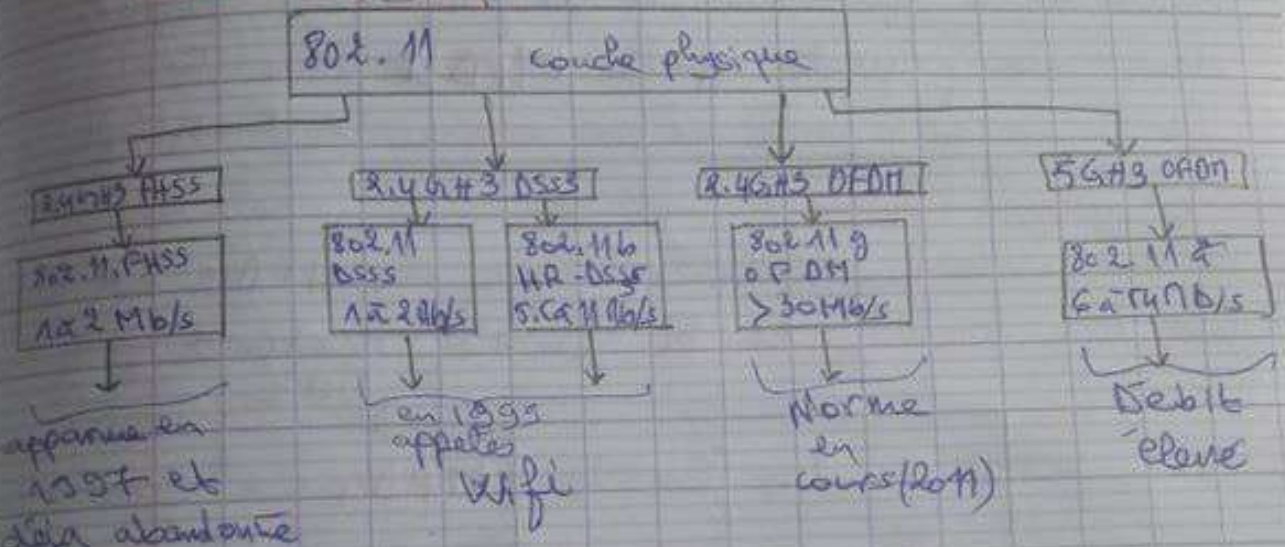
1 — phys, PMD

802,11 : IR, FHSS, DSSS, HR-DSSS (b), OFDM (a) 5GHz, OFDM (g) 2,4GHz

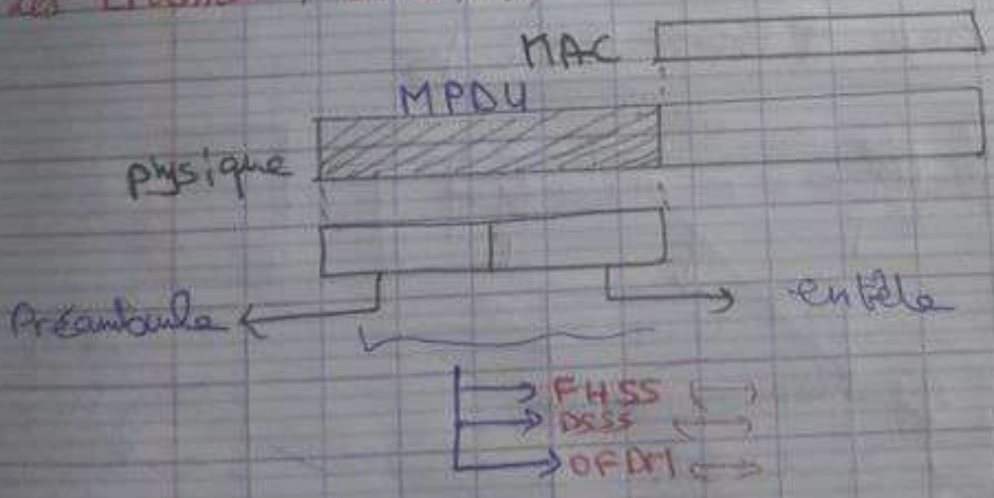
802.15 (1-4), Bluetooth, 802.15.4 Wireless HART, ...

4.2. la norme IEEE 802.11

La couche physique



les trames : 802.11

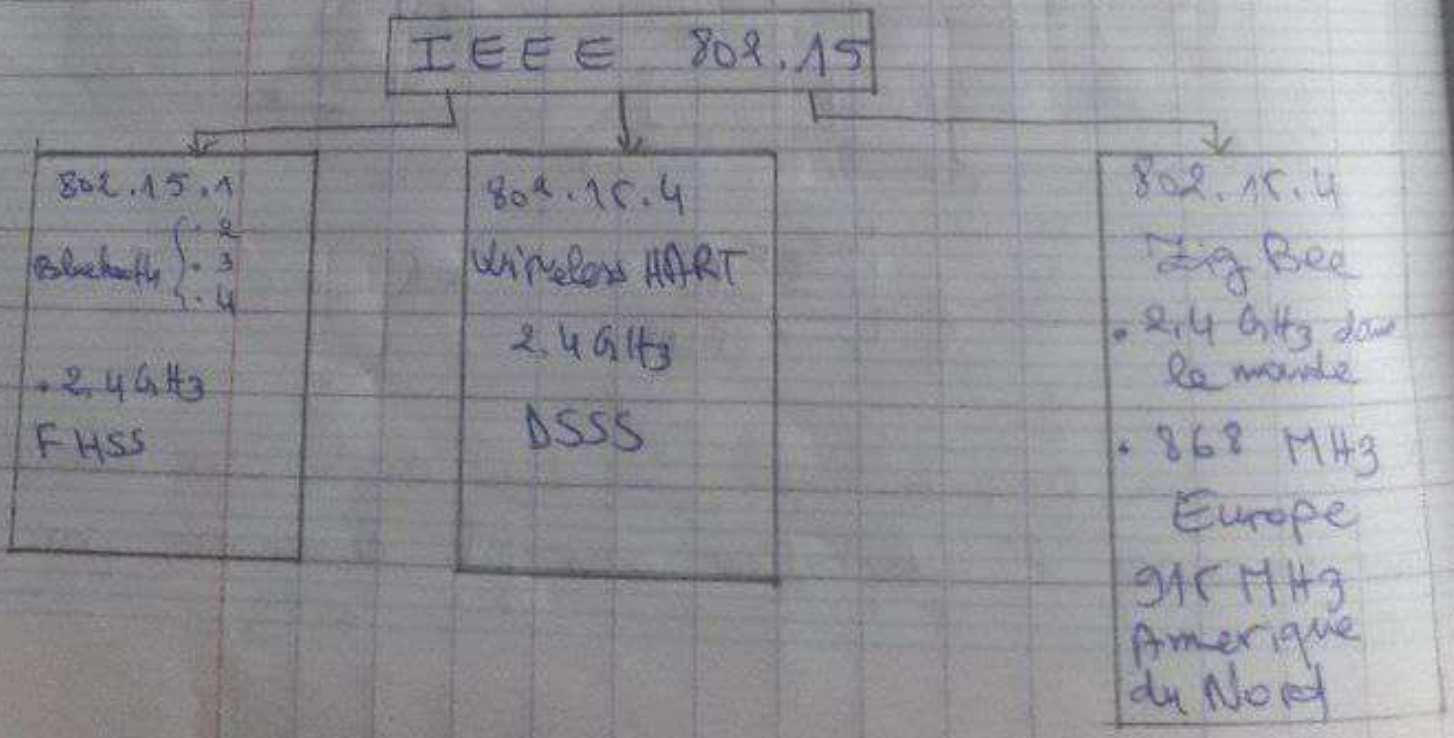


Lorsque un paquet de données doit être envoyé sur les ondes, l'adaptateur sans fil commence par le

traiter au niveau de la couche "mac". le paquet est eventuellement fragmenté, et les fragments sont encapsulés dans des paquets appelés MPDU (Mac Protocol Data Unit)

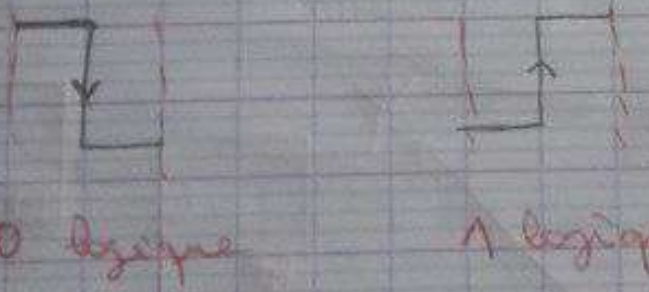
- Au niveau de la couche physique la MPDU est incluse dans une trame de la forme suivante

4.3 La norme IEEE 802.15



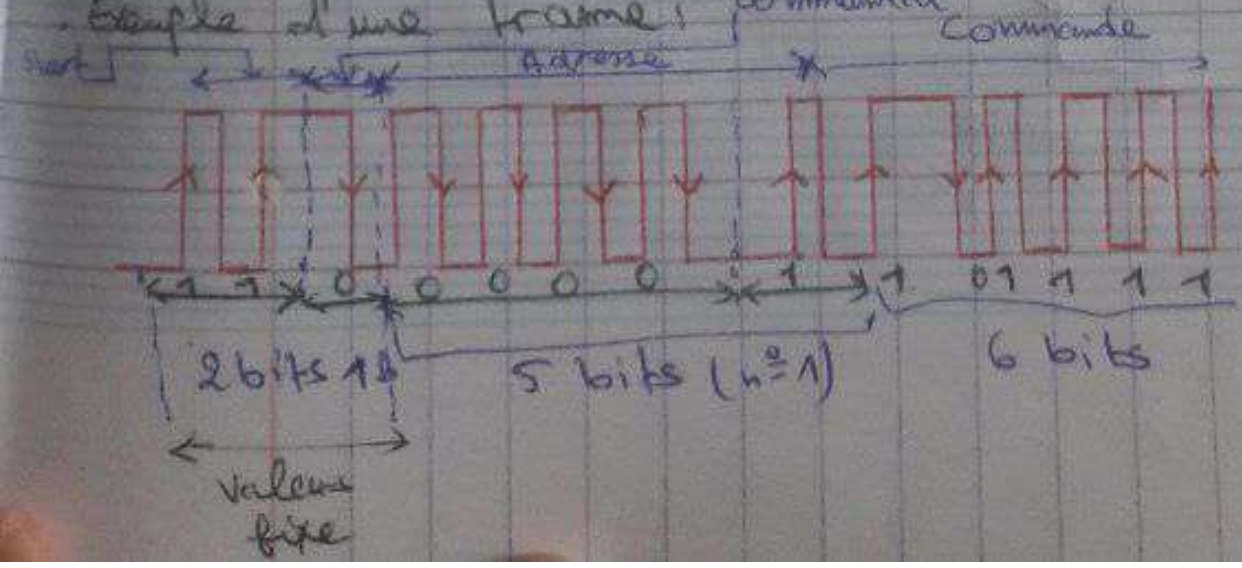
4.4. La norme 802.11 IR

La communication numérique basé sur le signaux infra-rouge (IR), est organisé sous plusieurs normes qui découle de la norme IEEE 802.11 IR. Parmis ces normes nous citons la norme RC5 developpé par la firme philips.
La lumière IR est émise par une LED. la modulation est réalisée avec une porteuse de 36KHz.
La trame RC5 est composée de 14 bits avec un codage manchester.



0 logique 1 logique

- Exemple d'une trame :



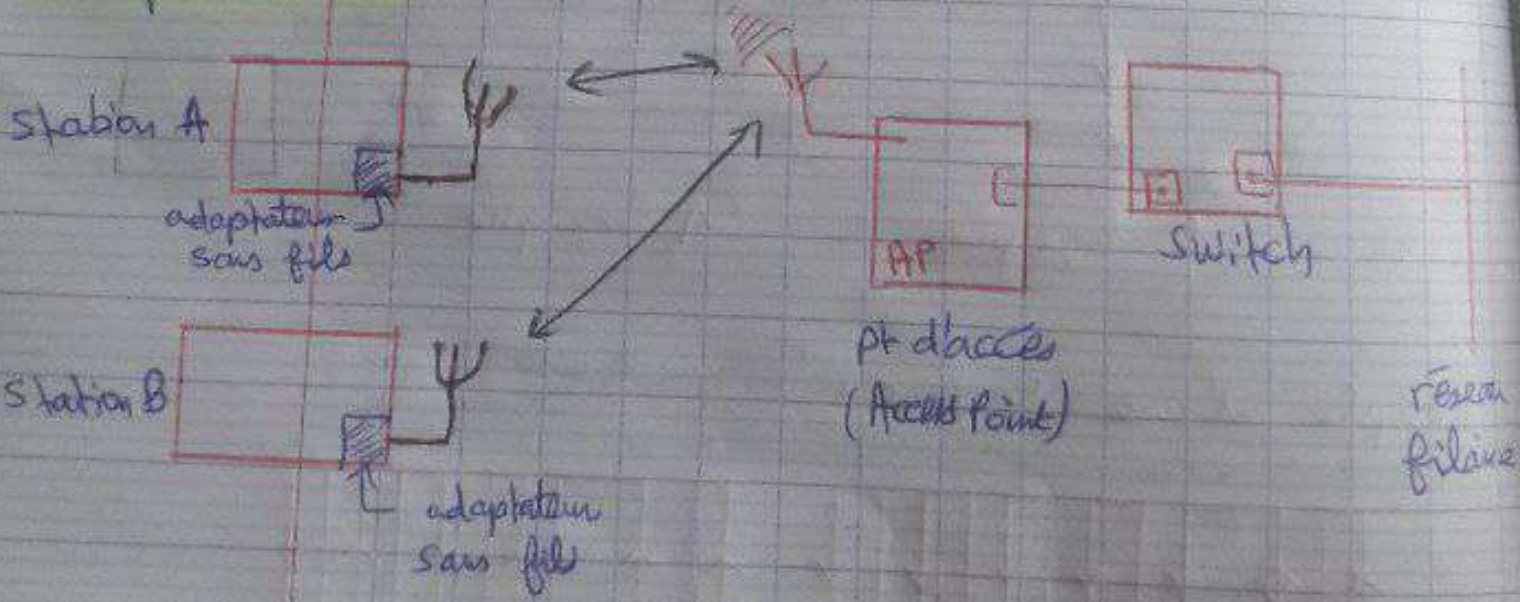
5. Les modes de fonctionnement des réseaux sans fils.

5.1. Les composants d'un réseau industriel sans fil:

a/ les adaptateurs:

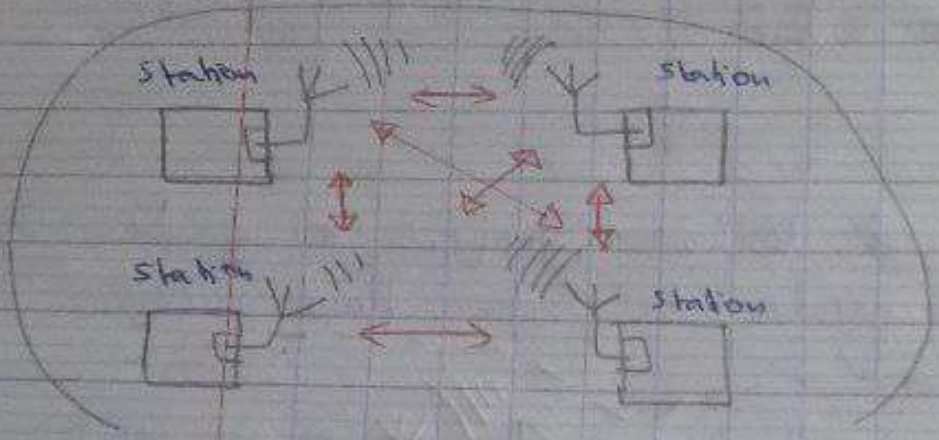
Les adaptateurs sans fil (ou carte d'accès) [wireless adapter / Network interface controler] est une carte réseau permettant à une machine de se connecter à un réseau sans fil.

b/ pt d'accès:



5.2 Les modes opératoires :

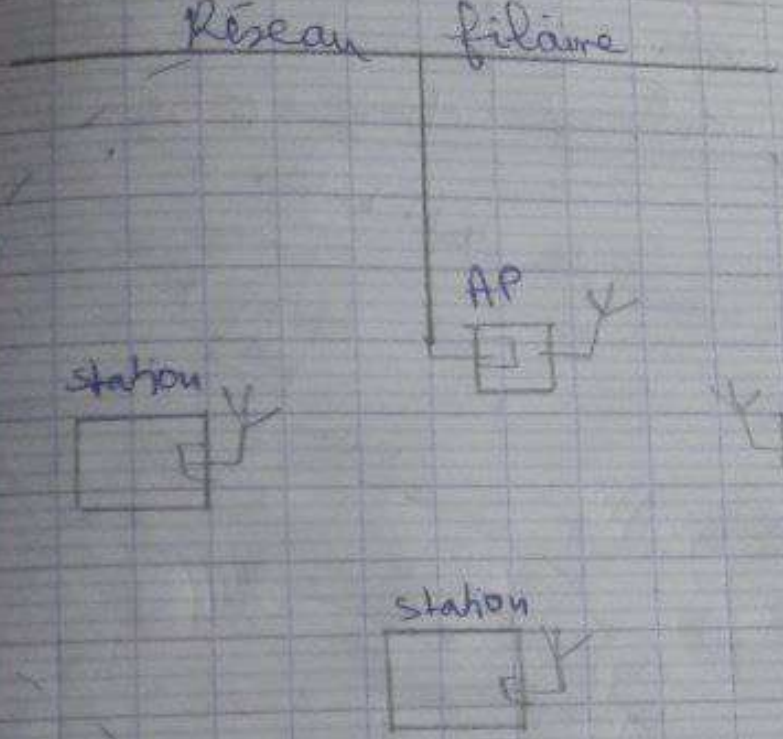
a- Le mode Ad-hoc :



Ensemble de service de base IBSS

Le mode Ad-Hoc, appelé également point à point, représente un ensemble de service de base indépendants. IBSS (Indépendant Basic Service Set). Dans ce mode l'ensemble des stations sans fil communiquent entre elles sans point d'accès ni connexion à réseau filaire.

b. le mode infrastructure BSS.

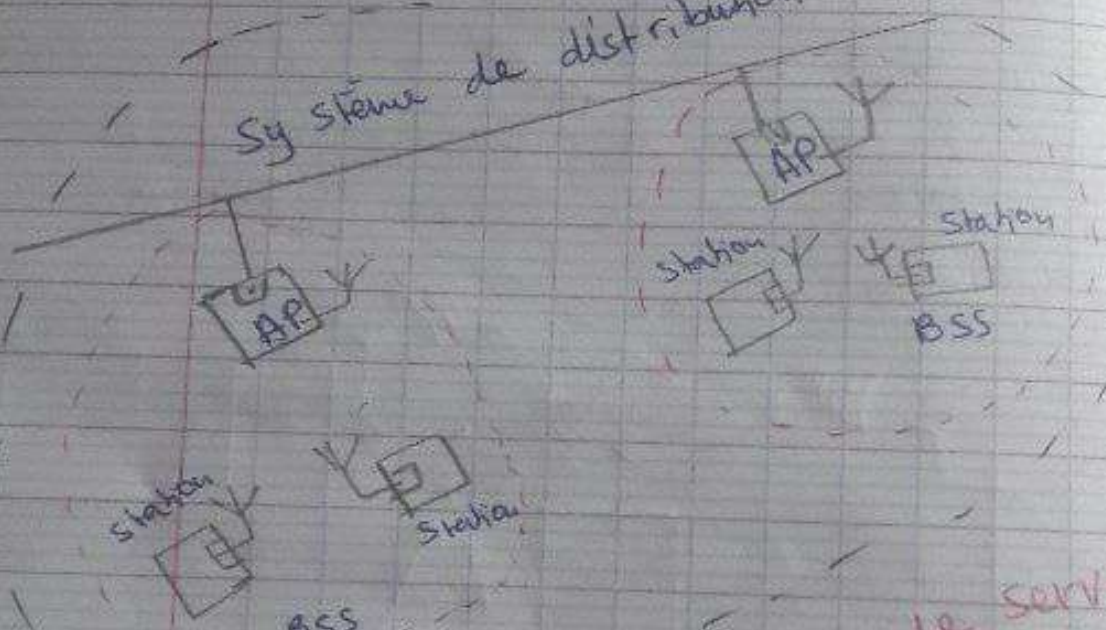


Ensemble de service de base BSS
(cellule unique)

Dans cette solution, le réseau sans fil consiste au minimum en un point d'accès = AP connecté à l'infrastructure du réseau filaire et un ensemble de station sans

fil. Cette configuration est notée :
Ensemble de service de base BSS
(Basic service set)

c- le mode infrastructure ESS :



ESS : Ensemble de service étendu

le syst de distribution peut être soit une infrastructure filaire ou une autre infrastructure sans fil.

6- Le protocole Wireless HART:

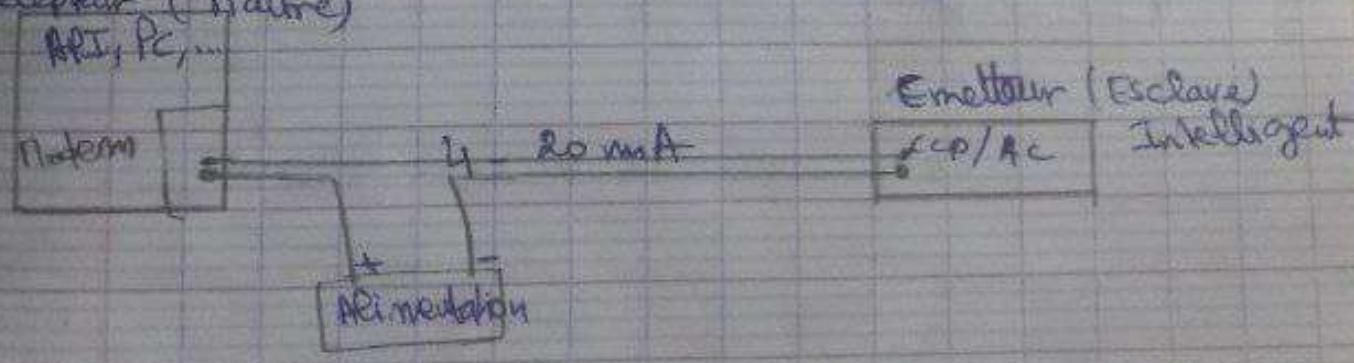
Wireless HART: Wireless Highway Addressed Remote Transducer

Le Wireless HART : Wireless Highway Addressed Remote Transducer

en français Transducer adressable à distance par voie sans fil.

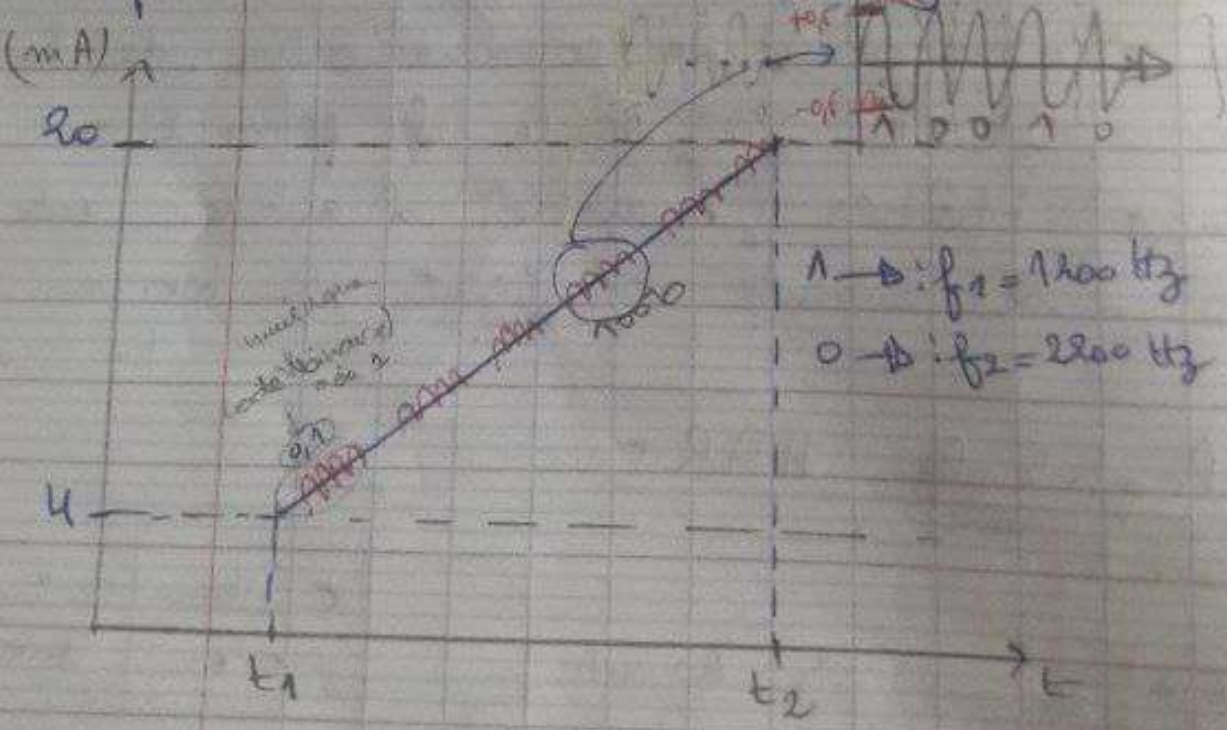
est un protocole de communication de la norme IEEE 802.15.4 il permet au systèmes Hôtes (maître) d'accéder aux données d'instruments intelligents de terrain

6-1- Protocole HART:

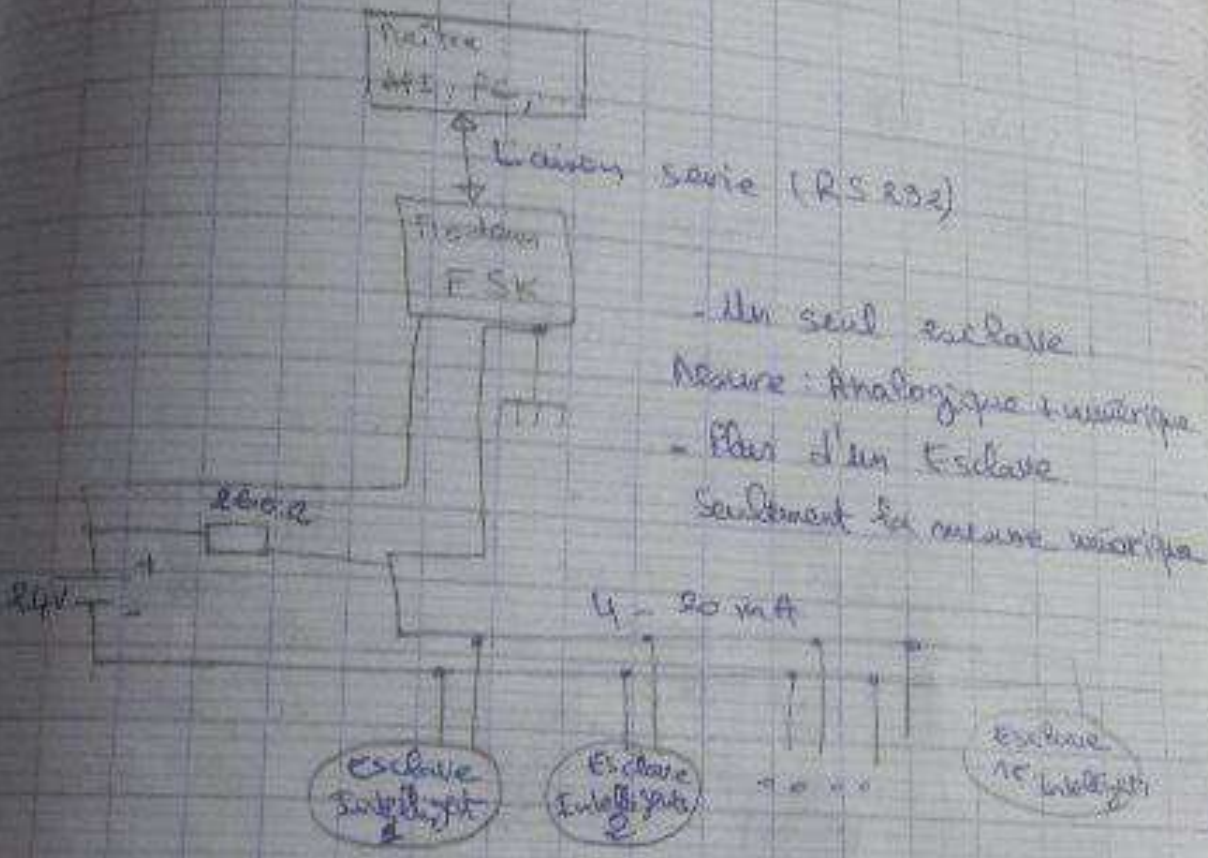


le protocole HART est implémenté sur une boucle 4 - 20 mA

+ Dans le protocole HART, le capteur classique est remplacé par un capteur intelligent.
+ La boucle analogique 4-20mA est conservée et la valeur mesurée peut être représentée par une valeur numérique.
+ Avec le protocole HART on peut accéder (à distance) aux données embarquées d'équipements (paramètres, configuration et diagnostic)
+ le protocole HART est de type Maître - Esclave



Liaison de raccordement à plusieurs esclaves

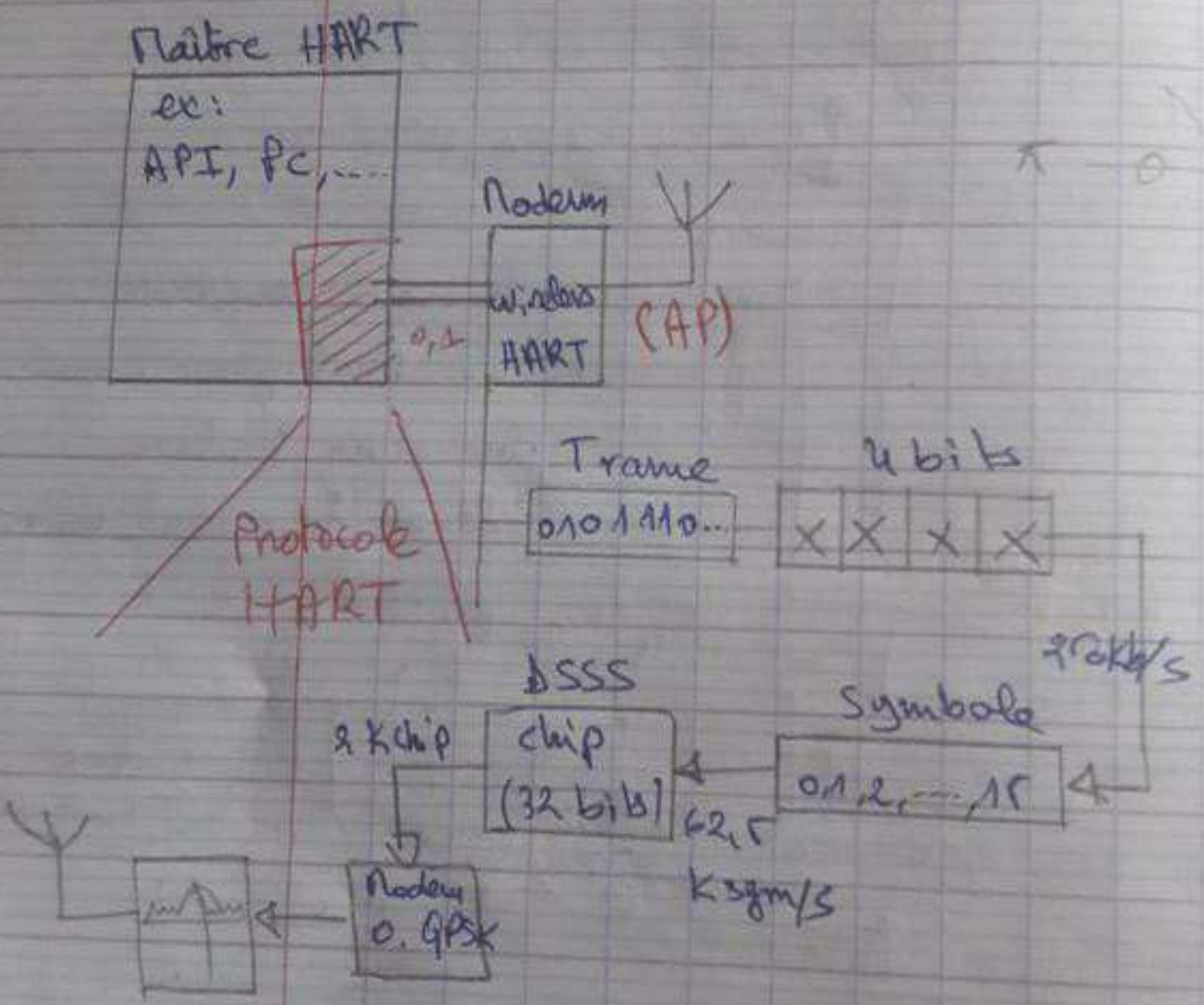


- La trame HART :

Préambule	Start	Adresse	Commande	BCNT (Longueur)	Données	Chk (contrôle)
2 octets	1 octet	5 octets	1 octet	1 octet	0 - 25 octets	1 octet

11 : lire le constructeur type de l'appareil.
1 : lire la variable primaire et l'unité (ex : Pression ; Bar)
36 : Réglage de la limite supérieure de la plage de mesure.

6.2. Le protocole wireless HART :



Chapitre 4 : Sécurité des réseaux de communication industrielle sans fil.

1. Introduction :

Afin d'obtenir un niveau de sécurité satisfaisant sur un réseau sans fil, il est nécessaire de connaître les vulnérabilités inhérentes à ce type de réseau.

- la diffusion de l'information facilitant l'interception passive à distance.
- la sensibilité au brouillage diminuant la disponibilité du réseau.
- les configurations non sécurisées par défaut des nouveaux équipements facilitent les attaques.

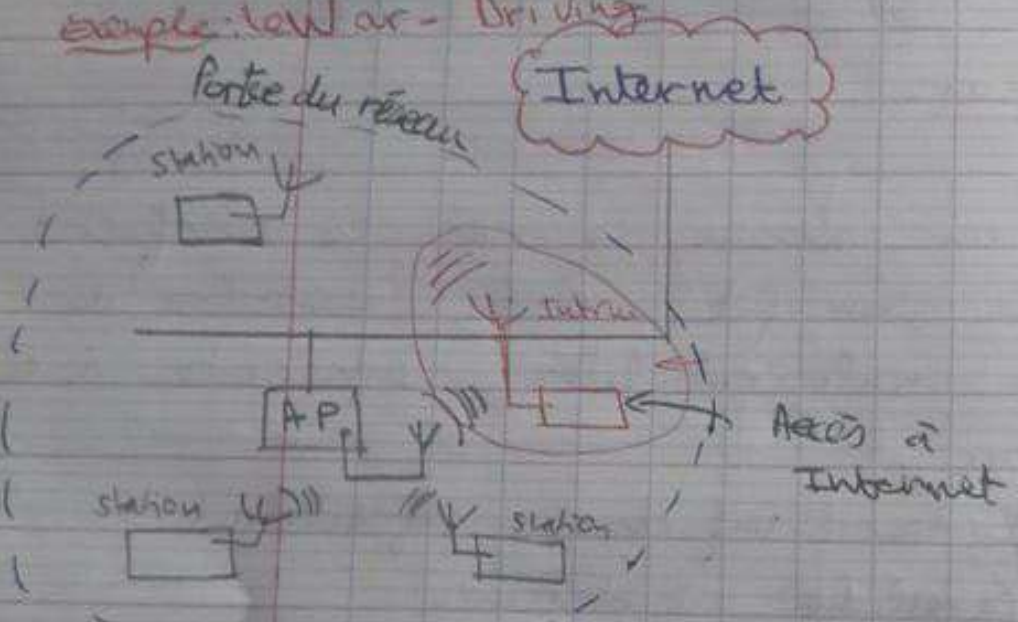
2. Les risques liés aux réseaux sans fil :

2.1. Le manque de sécurité :

Comme la transmission de données sans fil est basée sur ~~l~~ les ondes électromagnétiques et que ces dernières

se propagent dans toutes les directions, il y a une grande facilité d'écoute du réseau dans l'espace de sa portée.

Exemple: le War-Driving



Réseau non sécurié

le War-driving est un phénomène apparu aux USA il consiste à la recherche des réseaux sans fil pour obtenir un accès à Internet.

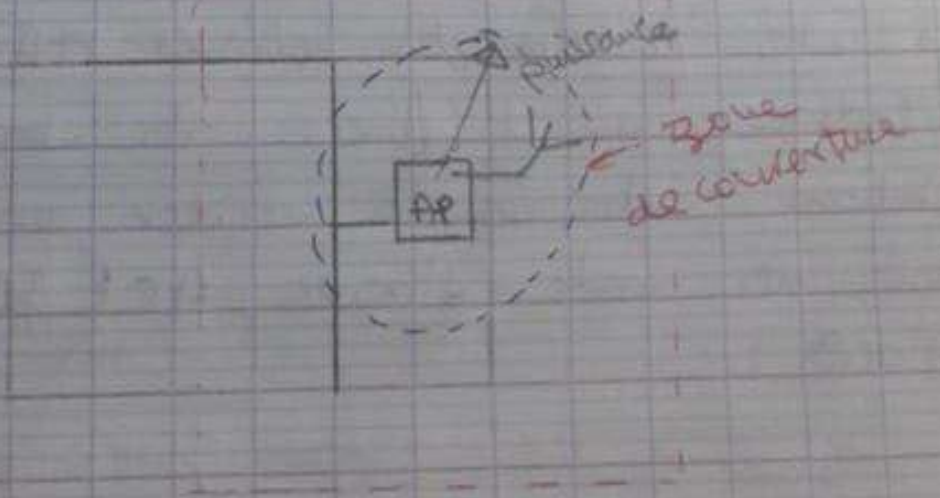
2.2 Les risques en matière de sécurité:

- les risque liés à la mauvaise protection d'un réseau sans fil sont:

- L'interception des données par écoute des transmissions.
- Le broillage des transmissions par emission sur le même canon de transmission
- le détournement de connexion pour obtenir un accès à un réseau local ou à Internet.
- les déni du service rendant le réseau inutilisable.
  - Soit en envoyant des commandes spéciales
  - = = = un très grand volume de données.

3- La sécurisation d'un réseau sans fil :

3.1 Adaptation de l'infrastructure



Régler la puissance et le positionnement des points d'accès selon la zone que l'on souhaite couvrir.

3.2. Eviter les valeurs par défaut :

Les valeurs du paramètre usine d'un point d'accès sont fixées pour un niveau de sécurité minimale. Par conséquent, après toute installation, il faut modifier les paramètres par défaut :

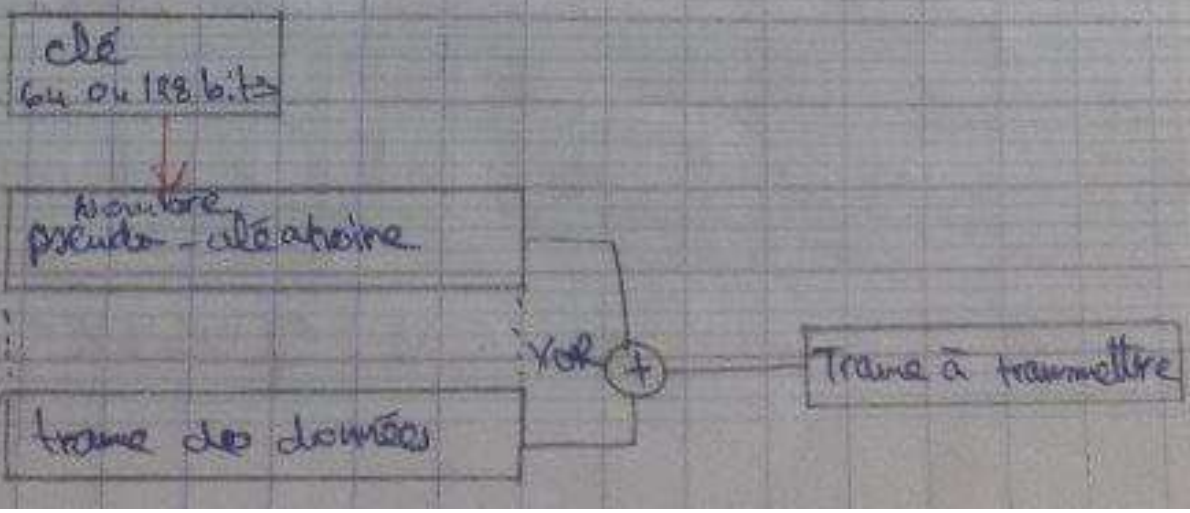
- modifier l'identifiant réseau. ID Réseau : SSID pour empêcher l'identification du type de l'appareil
- modifier le mot de passe administrateur.
- désactiver la diffusion broad cast.

3.3. Le filtrage des adresses MAC :

Indiquer au Pt d'accès les adresses MAC des stations autorisées à accéder au réseau (utiliser la liste des droits d'accès ACL disponibles sur le Pt d'accès).

3.4 Le WEP:

Le standard 802.11 intègre un mécanisme de chiffrement des données, il s'agit du WEP (Wired Equivalent Privacy)
Le WEP consiste à un chiffrement des trames en utilisant l'algorithme RC4 avec des clés d'une longueur de 64 bits ou de 128 bits.
Cette clé secrète doit être déclarée au niveau du pt d'accès et des clients (stations).
La clé sert à créer un nombre pseudo aléatoire d'une longueur égale à la longueur de la trame.
Chaque transmission de donnée est ainsi chiffré grace à un OU-Exclusif entre les données de la trame et le nombre pseudo aléatoire



- Principe de chiffrement :

exemple 1 : clé symétrique :

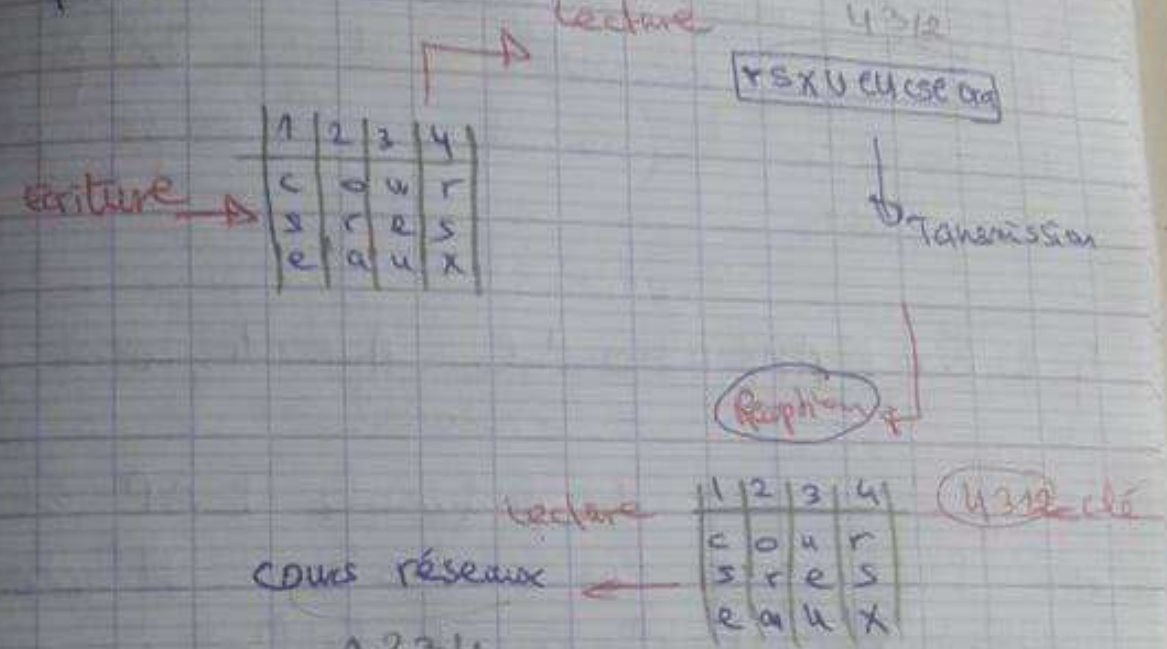
Translation des données par rapport à la clé

clé = 2, Données : AUTOMATIQUE

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A			•		•																					
U																					•					
T																				•						
O															•											
M													•													
A			•		•																					
T																				•						
I									•																	
Q																	•									
U																					•					
E					•																					

Not à transmettre : CWVQDCVKSWG

exemple : code à permutation (Modifier l'ordre des caractères selon une clé).
Données : cours réseaux
clé : 4312



4- Sécurisation avancée :
4.1 le WAP (Wifi Protected Access)

La WAP est une solution de sécurisation des réseaux sans fil, proposée par Wifi alience afin de combler les lacunes de WEP elle repose sur le protocole de criptage robuste.

TKIP (Tomporary Key Integrity Protocal)

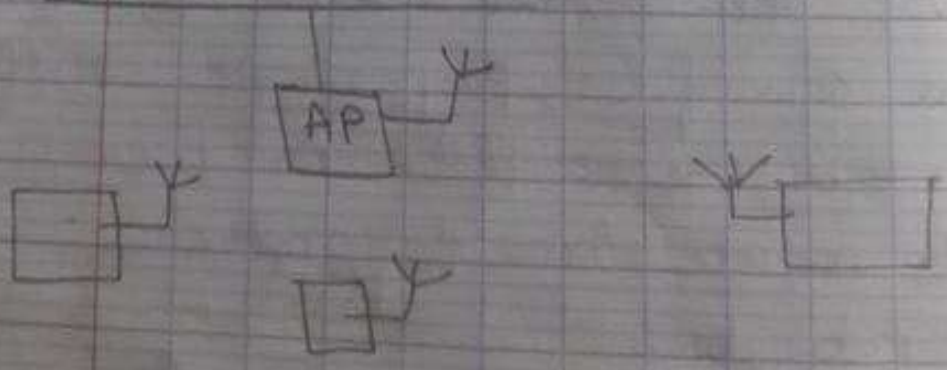
le TKIP permet la généralisation des clés d'une façon aléatoire etoffre la possibilité de modifier la clé dans le temps pour plus de sécurité.

4-2 La EAP(EXtensible Aithentifiation Protocal)

Le fonctionnement du protocole EAP est basé sur l'utilisation d'un contrôleur d'accès (Authentificateur) chargé d'établir ou non l'accès au réseau pour un utilisateur.

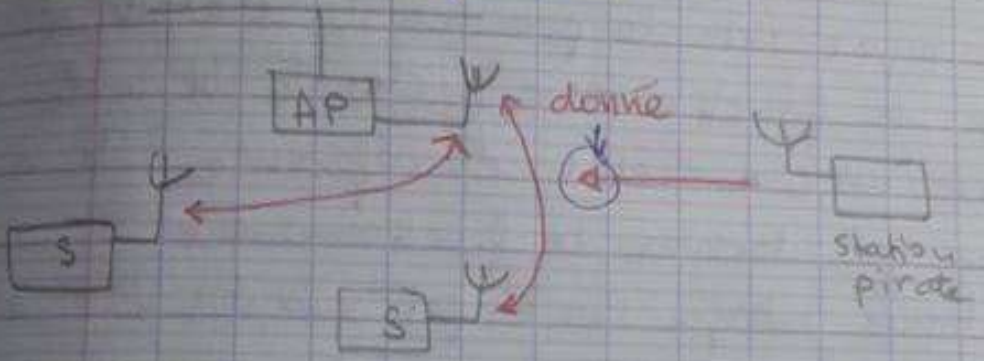
5- les differentes méthodes d'attaque :

5-1 le deni de service.



le pt d'accès sera occupé par une communication sans arrêt avec la station piraté.

5_2 le reniflage :



la station piraté analyse les données échangées par une station vers le pt d'accès afin de décoder les mots de passe embrouillés de chiffrement et donc accéder aux données process

5_3 L'usurpation informatique d'identité.

Cette technique consiste à obtenir l'adresse MAC d'une station ou d'un pt d'accès (disponible sur internet ou obtenue via une complicité) afin de modifier les paramètres de fonctionnement d'un processus.

Chapitre 15 : Diagnostiques de réseaux de communication industrielle.

1- Introduction :

le diagnostique est le processus d'evaluation d'un état de fonctionnement donné si cette état est comparé avec un état de référence, Il s'agit d'évaluation de derives de fonctionnement.

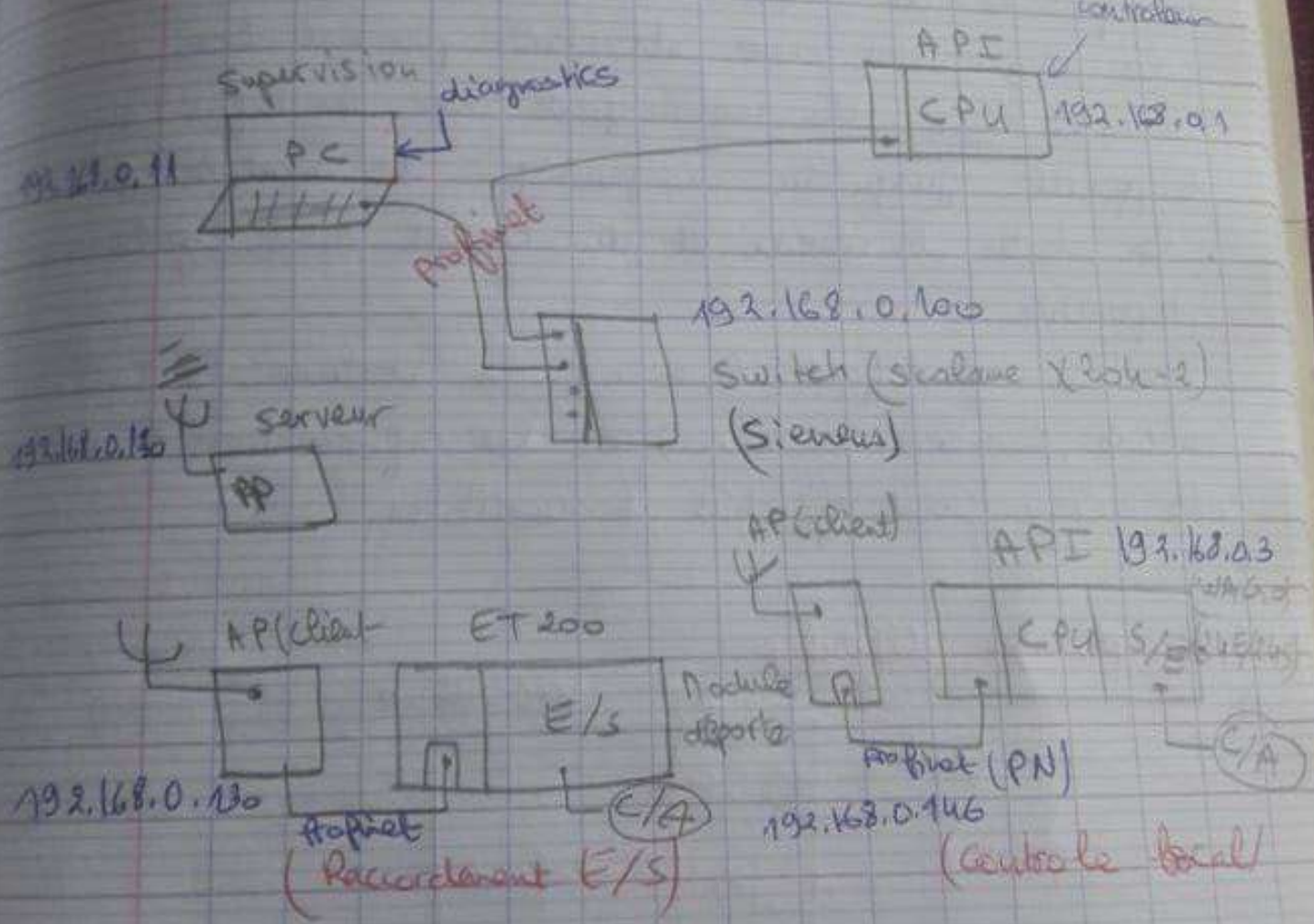
le diagnostique integre les étapes suivantes :

- Detection de cet etat de fonctionnement.
- Evolution des causes de cet état de fonctionnement consiste à identifier, analyser et localiser ces causes.
- decision d'action pour modifier cet état de fonctionnement.

L'objectif du diagnostique est :

- Diagnostic de bon ou mauvais fonctionnement.
- Diagnostic de panne ou défaillance.
- " de performance ou non performance.
- " d'erreur humaine ou fiabilité.

2- Exemple : Réseau Profinet.

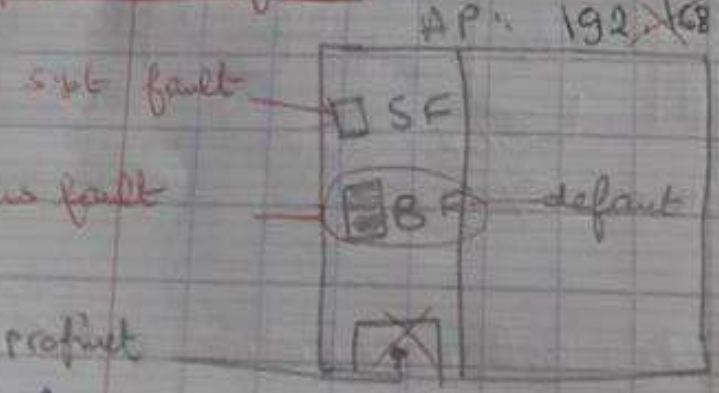


Type : Node infrastructure BSS

- Profinet fournit des diagnostics couvrant tous les composants du réseau.
- Les diagnostics sont structurés par manière Hiérarchique. On commençant avec les infos sur l'appareil jusqu'au diagnostique de module et de canal
- le statut du réseau et du canal sont également disponible.
- En cas de défaut le nom de la station, le numéro du module, numéro du canal et les informations sur l'erreur elle même sont affichés et accessibles.

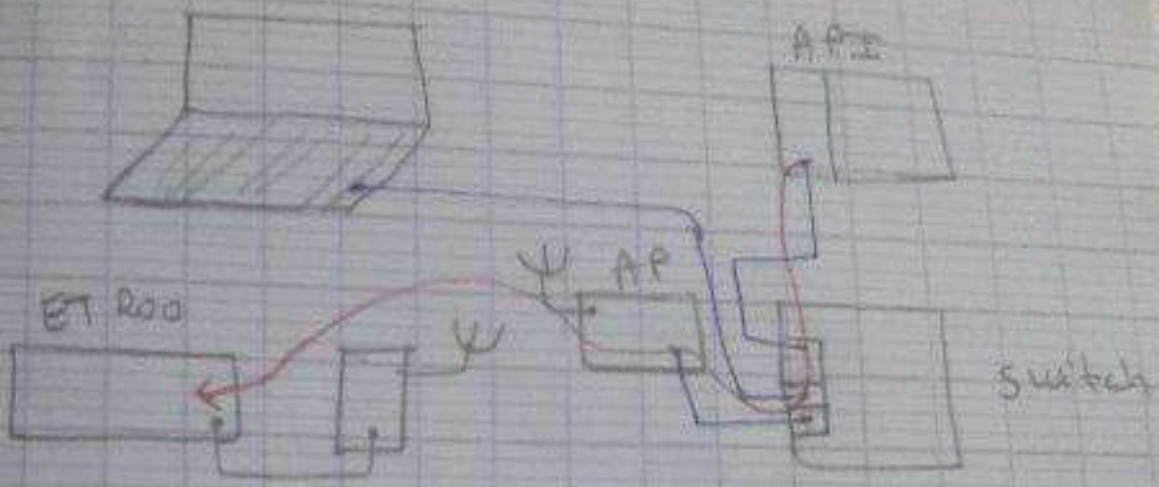
Exemple de défauts:

1)



principalement causé par un mauvais cablage (mauvaise configuration) ou de déterioration du cable réseau.

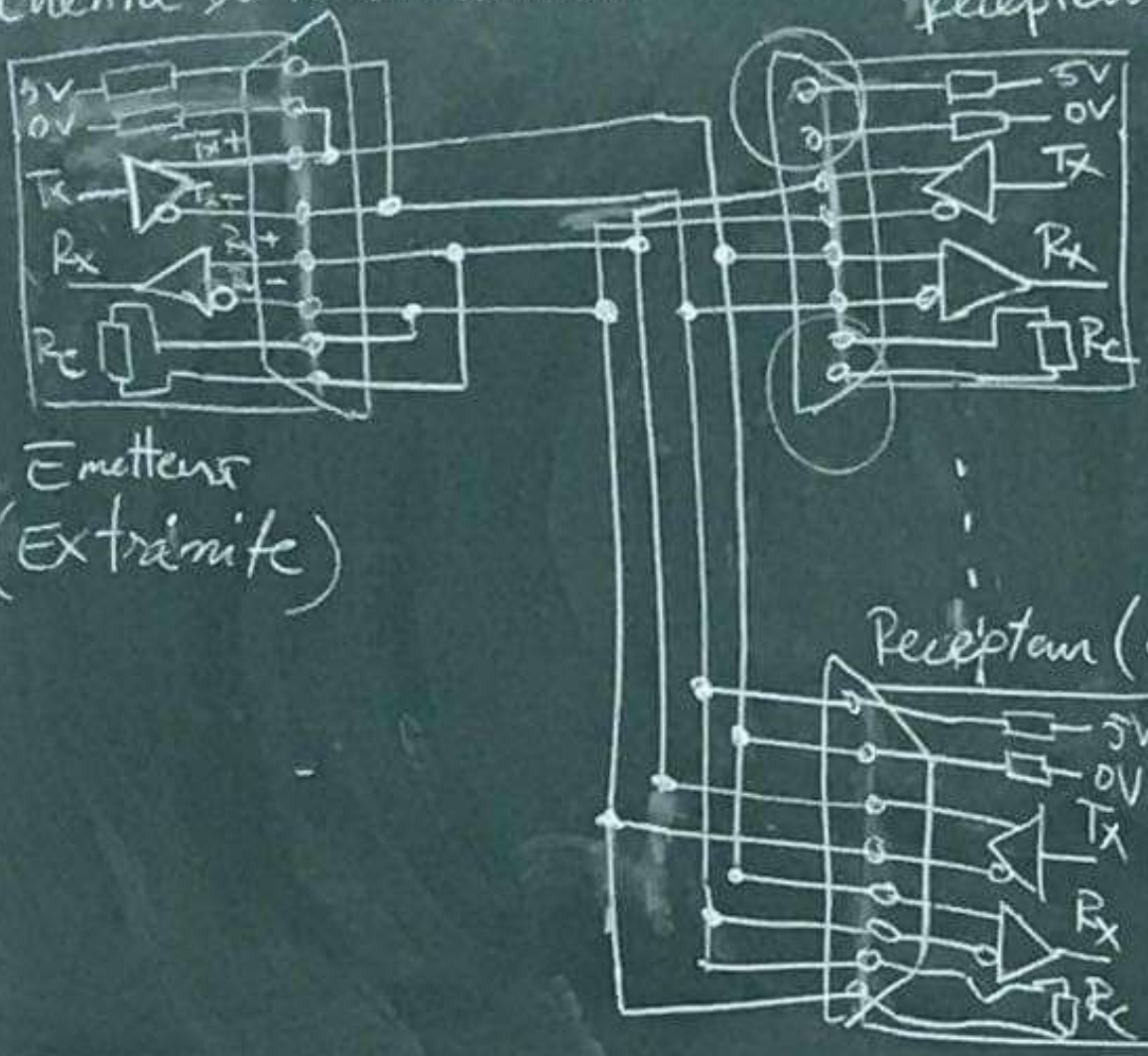
2)



- Switch transmet le diag du module ET 200
- L'API evalue et rapporte les diagnostiques. le switch signale au PC les perturbations du réseau autant que le diagnostic Profinet au module ET 200.

le PC indique le type de défaut et les solutions possibles.

_Schéma de raccordement



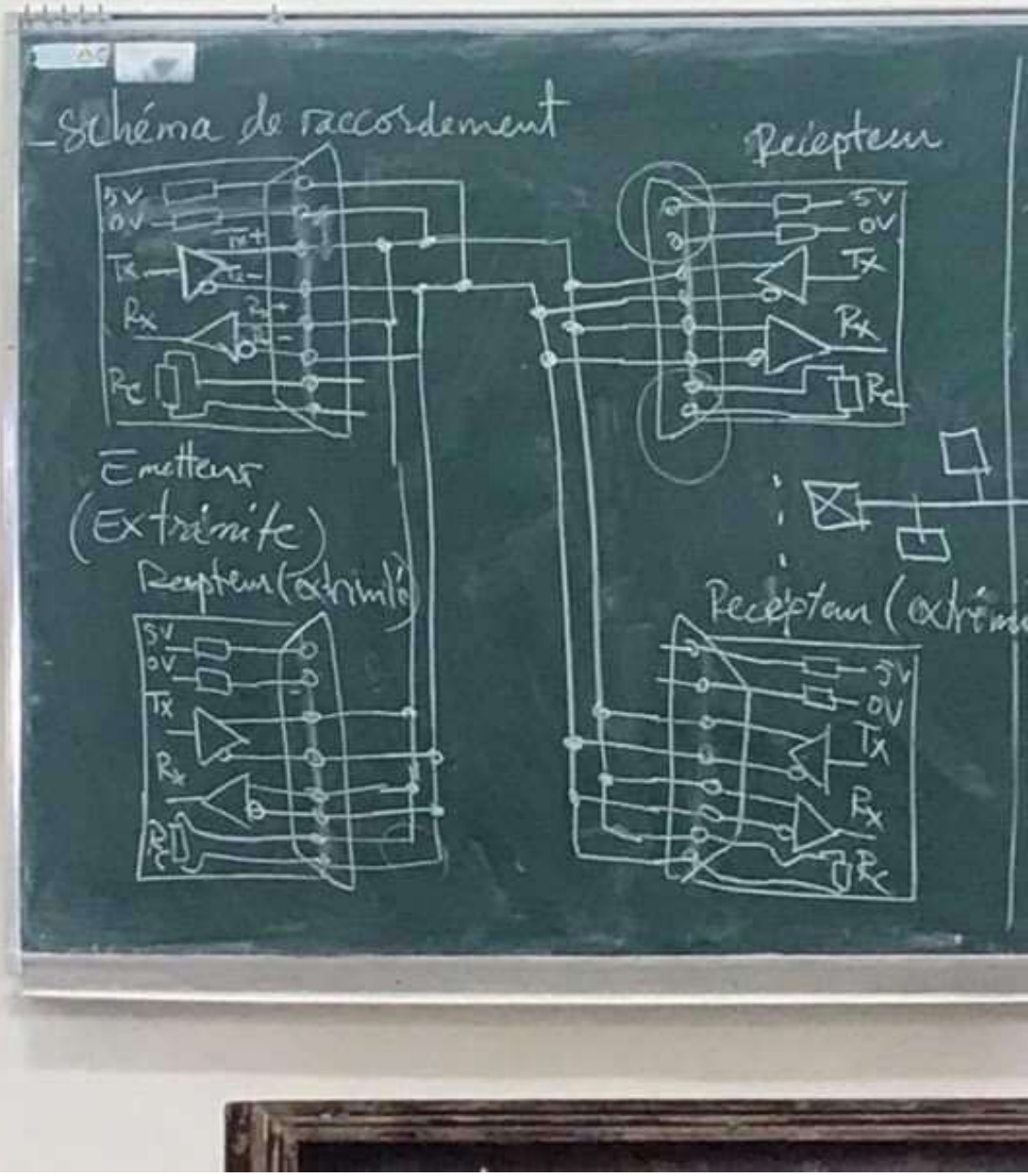


_Schéma de raccordement
Récepteur
5V
0V
Tx
Rx
Rc
Emetteur
(Extrémité)
Recepteur (extrimité)
Récepteur (extrémité)