

# Réseaux II (L3 2018-2019)

Troisième partie

jean.connier@uca.fr

Couche 2, suite

## Couche 2, suite

Deux exemples de protocoles de couche 2.

- ▶ ***SLIP***
- ▶ ***PPP***

## Couche 2, suite

Rappel : déjà vu **MAC** et **LLC** (Ethernet / suite 802).  
C'était malheureusement peu clair.

## Couche 2, suite

Donc, SLIP et PPP.

Couche 2 : SLIP

## Couche 2 : SLIP

***SLIP : Serial Line Internet Protocol***

RFC 1055 :

“A NONSTANDARD FOR TRANSMISSION OF IP DATAGRAMS  
OVER SERIAL LINES: SLIP”

## Couche 2 : SLIP

Très simple :

- ▶ 1 paragraphe d'introduction
- ▶ 3 paragraphes d'historique
- ▶ 2 paragraphes pour dire où trouver le pilote
- ▶ 3 paragraphes de protocole
- ▶ 6 paragraphes de limitations

et une implémentation en 127 lignes de C

## Couche 2 : SLIP

Utilité : encapsuler des **paquets** IP et les envoyer sur port série.

Il faut :

- ▶ Pouvoir reconnaître le début et la fin d'un paquet ;
- ▶ C'est tout.

## Couche 2 : SLIP

Comment reconnaître le début/la fin d'un paquet ?

## Couche 2 : SLIP

On insère un marqueur.

Dans SLIP, il s'appelle **END** :

```
#define END      0300 /* indicates end of packet */
```

... et il indique le début aussi

## Couche 2 : SLIP

Donc :

1. On envoie *END*
2. On envoie le message
3. On envoie *END*

Problème ?

## Couche 2 : SLIP

... Et si le message contient ***0xC0*** ?  
*(0xC0 == 0300 == 192 == END)*

## Couche 2 : SLIP

Solution ?  
Transformer ?

## Couche 2 : SLIP

Échappement !

Comme '\ en C et dans à peu près tous les langages.

## Couche 2 : SLIP

```
#define ESC          0333 /* indicates byte stuffing */
#define ESC_END       0334 /* ESC ESC_END means END data byte */,
#define ESC_ESC        0335 /* ESC ESC_ESC means ESC data byte */
```

## Couche 2 : SLIP

En hexadécimal...

```
#define END      0300 /* 0xC0 */
#define ESC       0333 /* 0xDB */
#define ESC_END   0334 /* 0xDC */
#define ESC_ESC   0335 /* 0xDD */
```

## Couche 2 : SLIP

Exemple : on veut envoyer le message :

0x63 0x65 0x63 0x69 0xc0 0x65

J'imagine que ça n'est pas un paquet IP valide mais oublions IP pour l'exemple.

## Couche 2 : SLIP

MESSAGE : **63|65|63|69|CO|65**

Figure 1:

## Couche 2 : SLIP

MESSAGE : **63|65|63|69|CO|65**

SLIP:

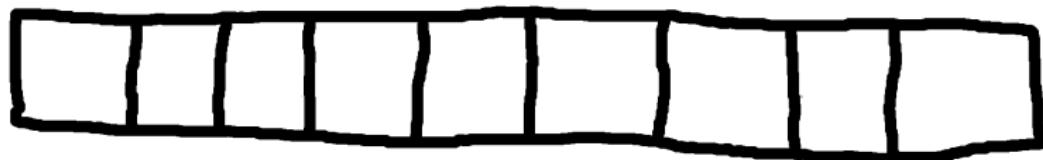


Figure 2:

## Couche 2 : SLIP

MESSAGE : **63|65|63|69|CO|65**

SLIP:

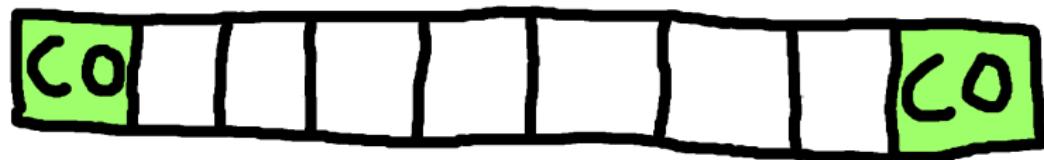


Figure 3:

## Couche 2 : SLIP

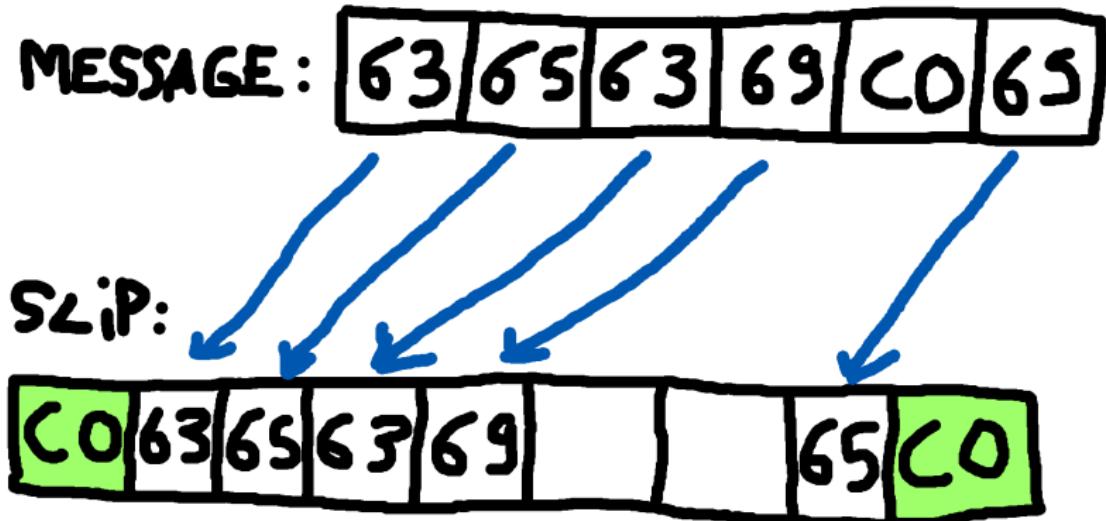


Figure 4:

## Couche 2 : SLIP

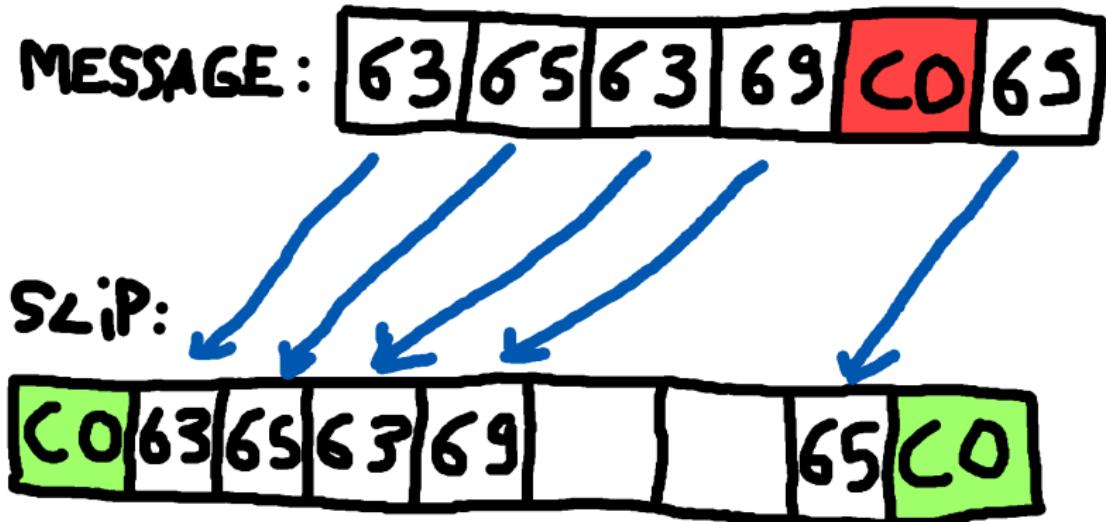


Figure 5:

## Couche 2 : SLIP

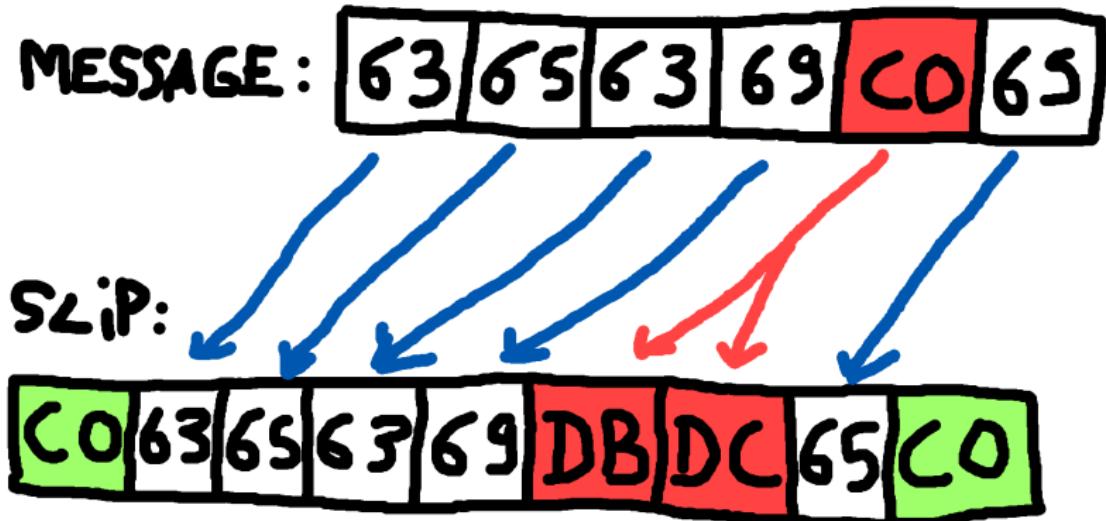


Figure 6:

## Couche 2 : SLIP

Et si il y a ***0xDB 0xDC*** dans le message ?

## Couche 2 : SLIP

MESSAGE : **(PAS GLOP)** 

Figure 7:

## Couche 2 : SLIP

MESSAGE : **CO DB DC DC DB**  
**(PAS GLOP)**



Figure 8:

## Couche 2 : SLIP

MESSAGE : CO DB DC DC DB  
(PAS GLOP)



Figure 9:

## Couche 2 : SLIP

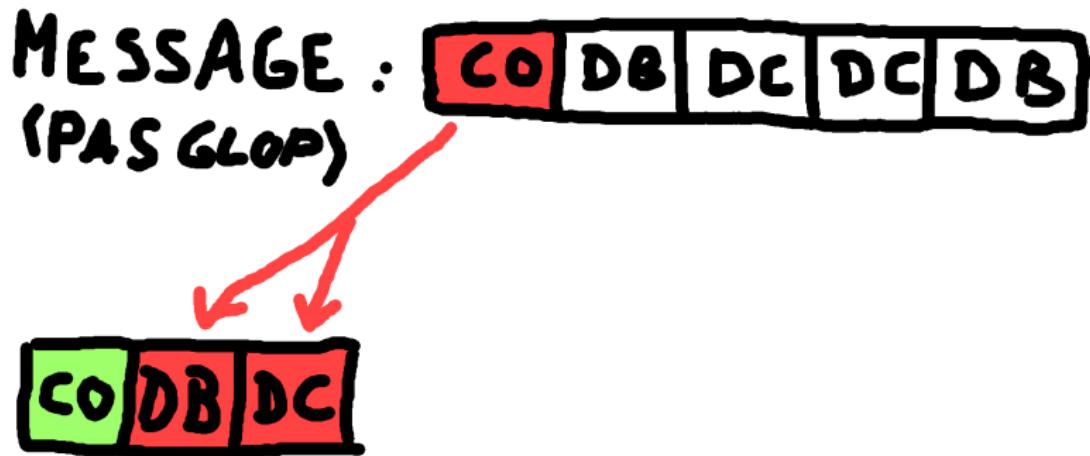


Figure 10:

## Couche 2 : SLIP

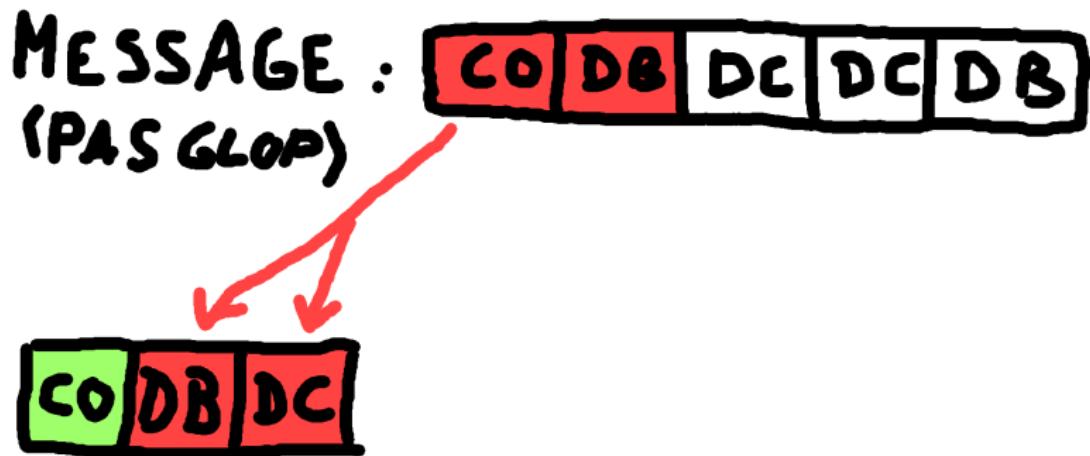


Figure 11:

## Couche 2 : SLIP

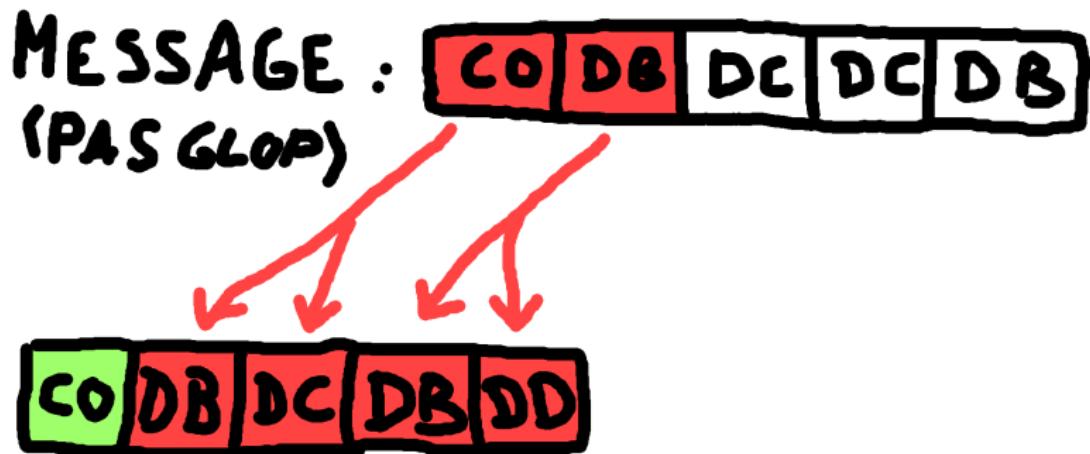


Figure 12:

## Couche 2 : SLIP

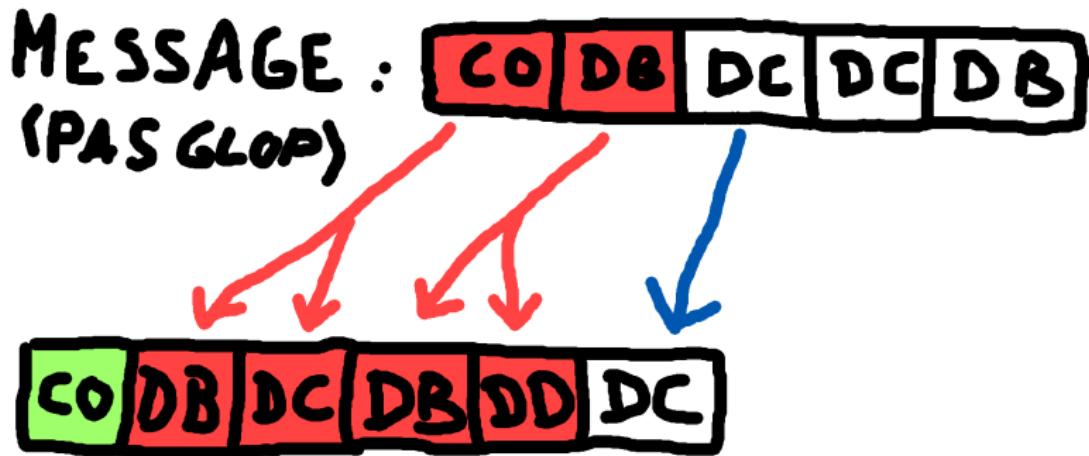


Figure 13:

## Couche 2 : SLIP

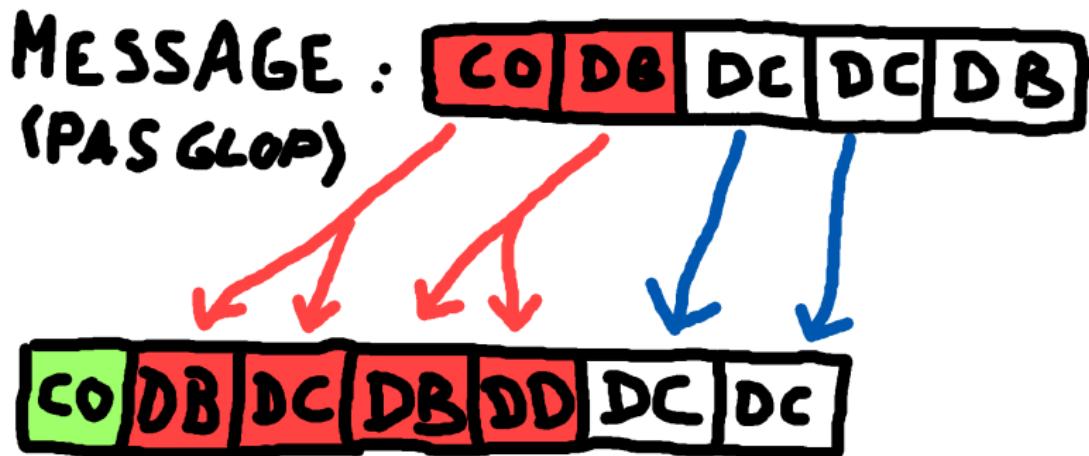


Figure 14:

## Couche 2 : SLIP

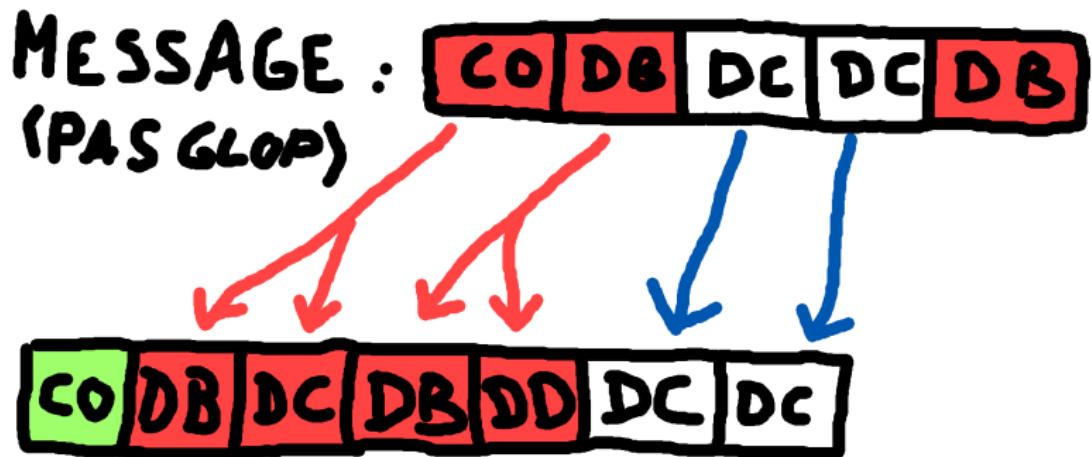


Figure 15:

## Couche 2 : SLIP

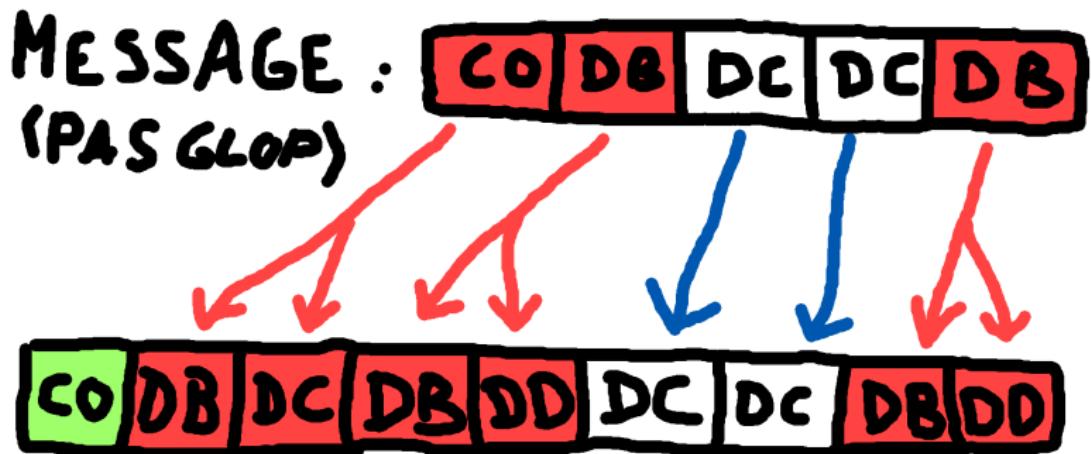


Figure 16:

## Couche 2 : SLIP

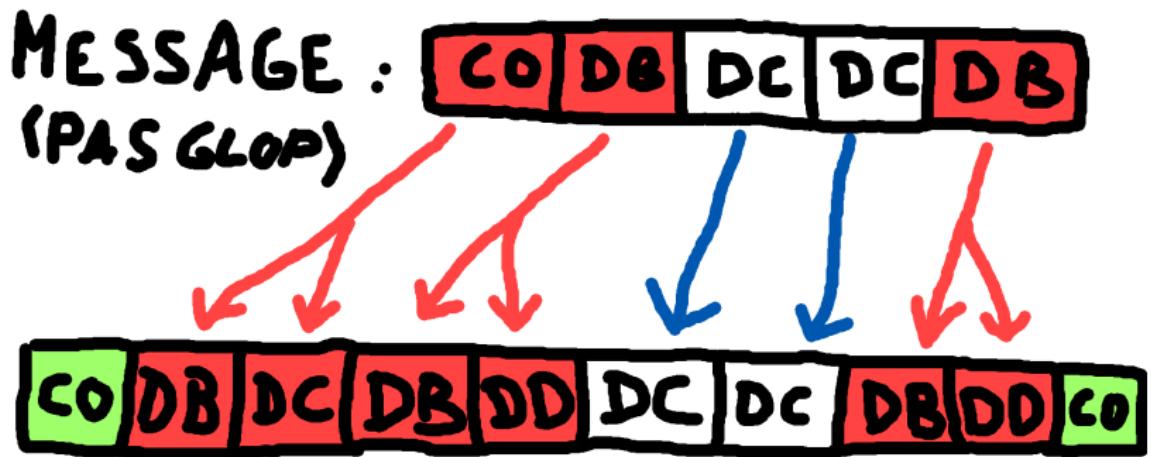


Figure 17:

## Couche 2 : SLIP

Algorithme de lecture ?

## Couche 2 : SLIP

Taille de trame SLIP : souvent, 1006 o, mais pas défini formellement.

## Couche 2 : SLIP

Voilà, c'était SLIP.

## Couche 2 : SLIP

Quelques problèmes de SLIP :

- ▶ Pas de mécanisme pour connaître l'adresse IP de l'autre (style ARP/RARP)
- ▶ Pas d'identificateur de protocole encapsulé => encapsulation d'un seul protocole (pas de multiplexage)
- ▶ Détection d'erreur ?
- ▶ Compression ? (il y a quand même une version compressée, CSLIP)

Couche 2 : PPP

## Couche 2 : PPP

***PPP = Point to Point Protocol***

Évolué !

## Couche 2 : PPP

Fonctionnalités :

- ▶ Authentification
- ▶ Chiffrement
- ▶ Compression
- ▶ Autres fonctionnalités

## Couche 2 : PPP

*PPP* est donc un protocole un peu complexe.

Il est séparé en plusieurs parties/sous-protocoles (et plusieurs *Requests For Comments/RFCs*).

Il est “extensible”.

## Couche 2 : PPP

1. Encapsulation, multiplexages : trames (la base) ;
2. **Link Control Protocol (*LCP*)** ;
3. **Des Network Control Protocols (*NCPs*)** ;
4. **Des protocoles de support de *LCP*** ;
5. **Des protocoles optionnels de *LCP*.**

Chaque partie a ses *RFCs*.

## Couche 2 : PPP

Commençons par LCP (on décrira les trames plus tard) :  
LCP gère le ***lien*** (merci captain obvious).

## Couche 2 : PPP

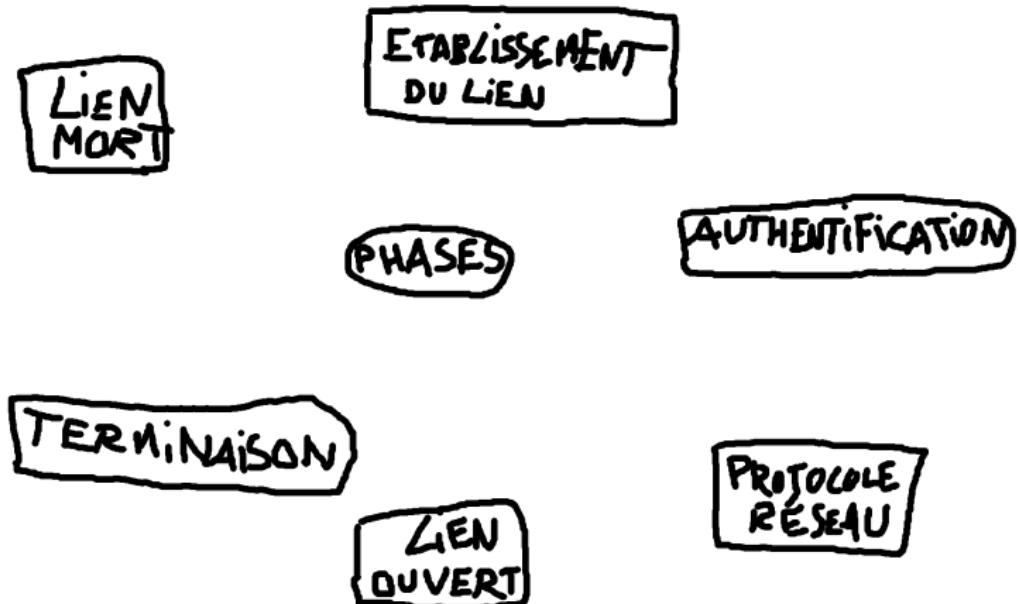


Figure 18:

## Couche 2 : PPP

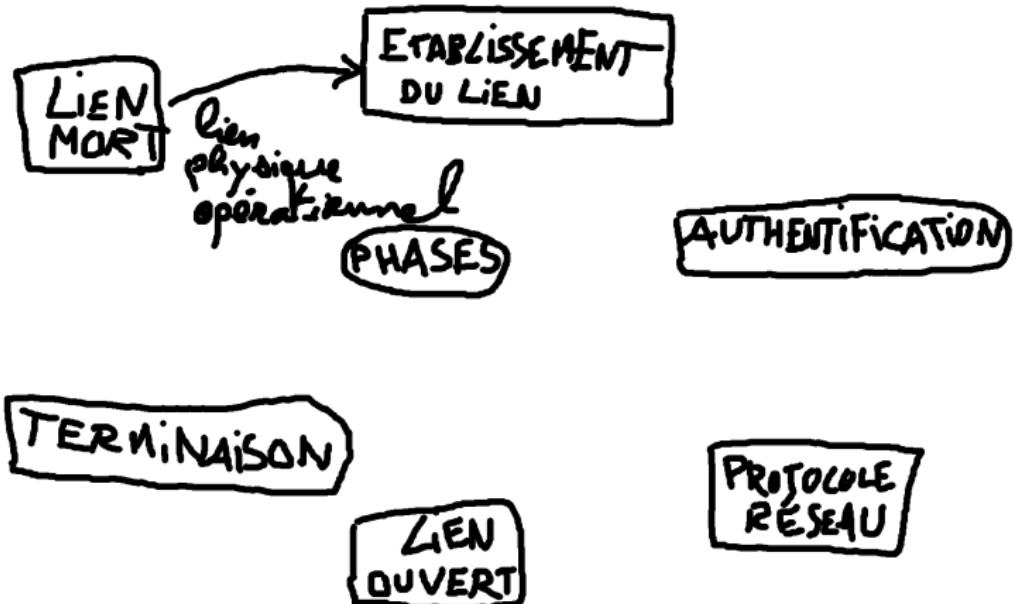


Figure 19:

## Couche 2 : PPP

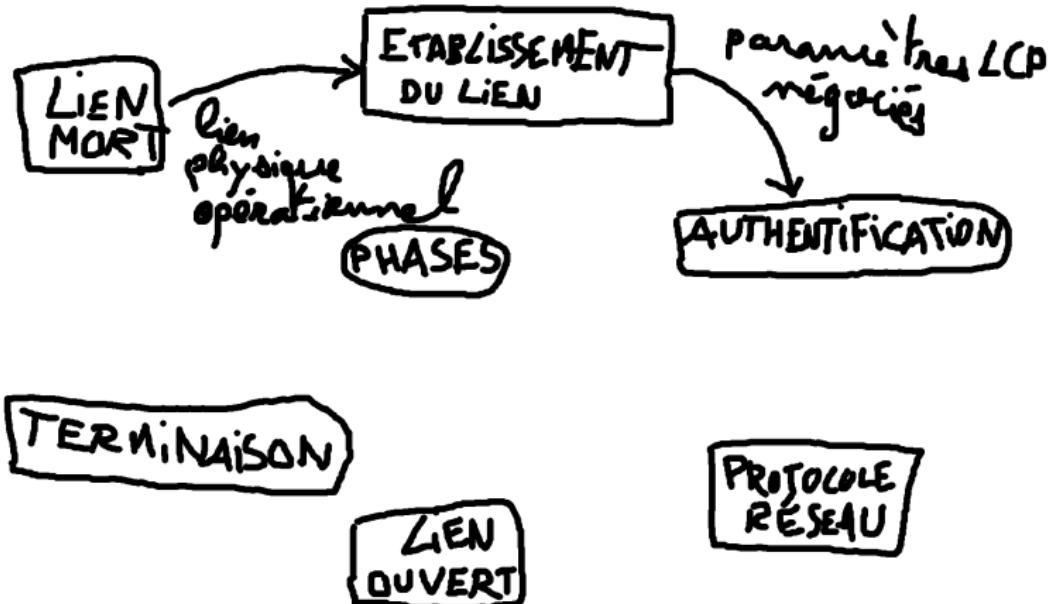


Figure 20:

## Couche 2 : PPP

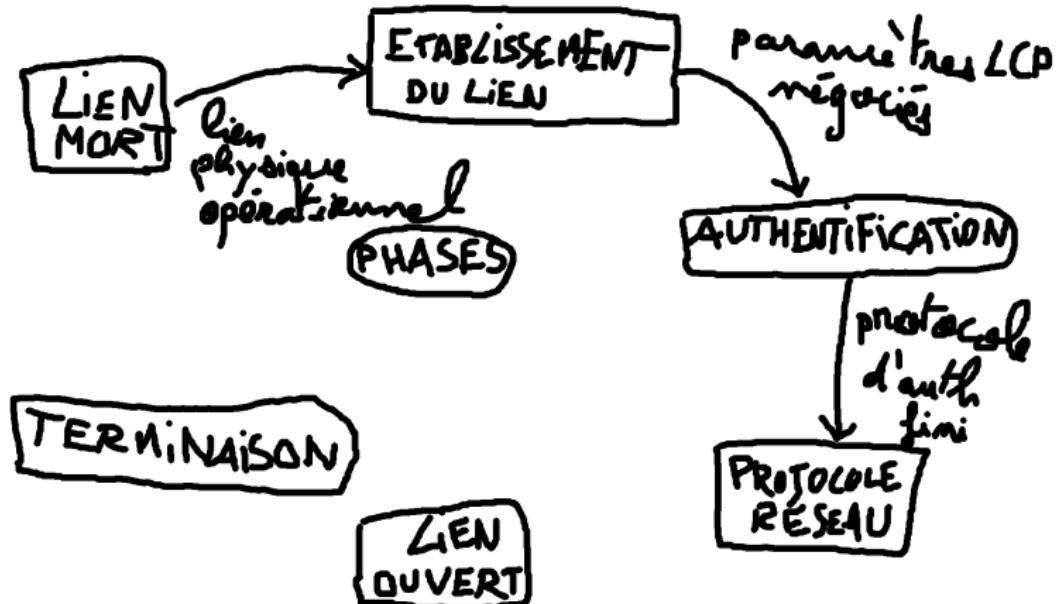


Figure 21:

## Couche 2 : PPP

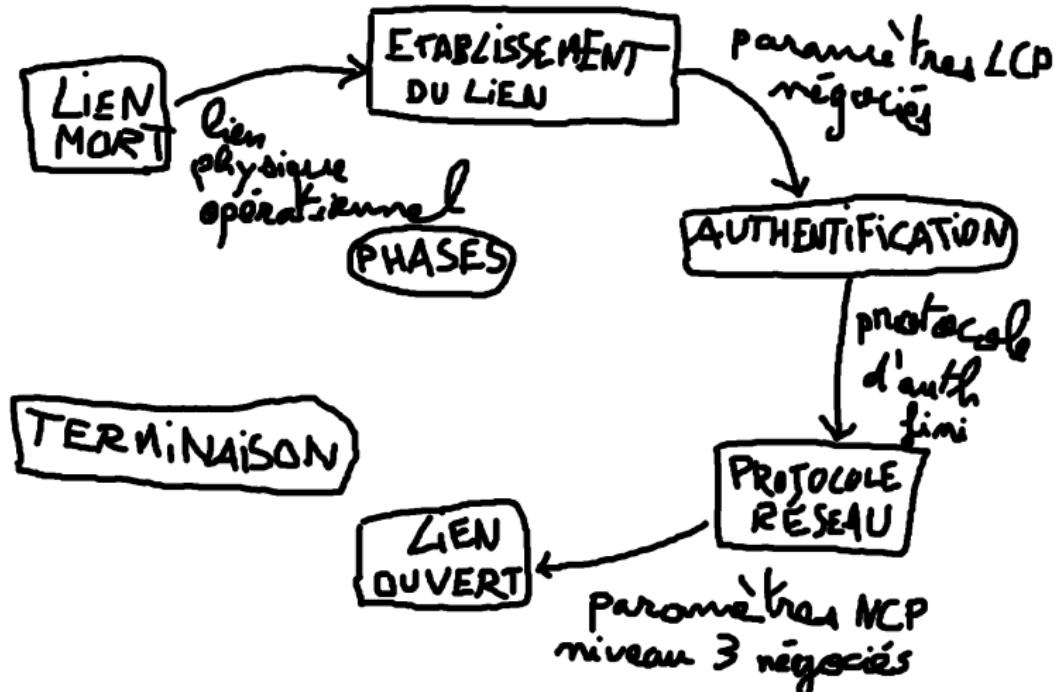


Figure 22:

## Couche 2 : PPP

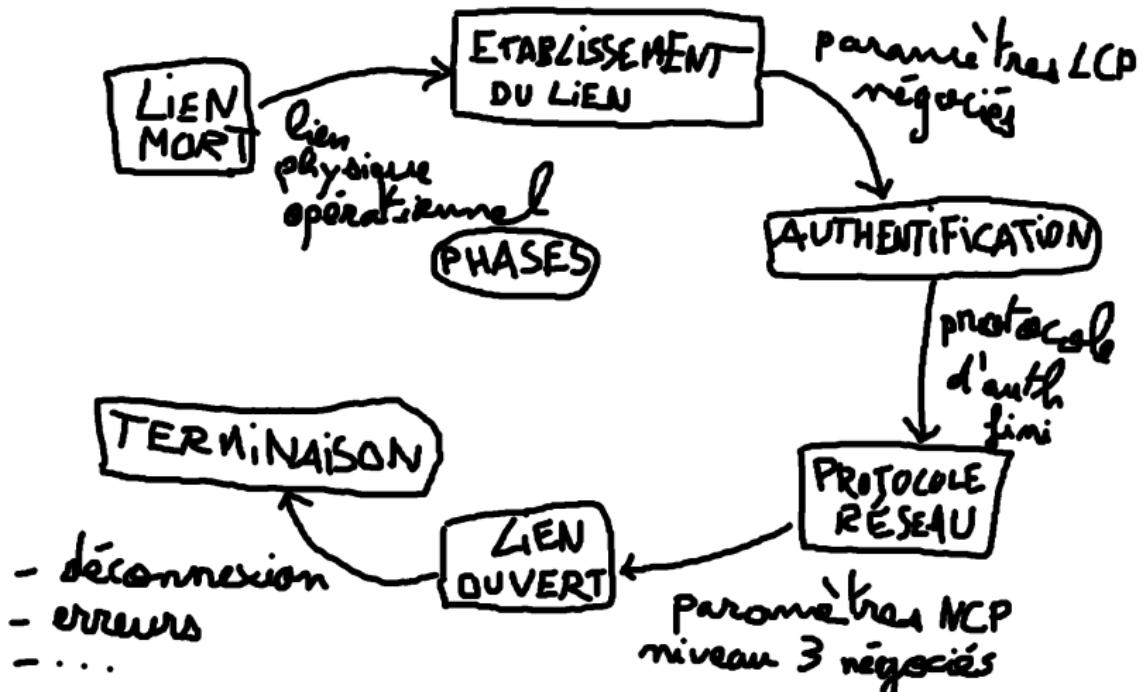


Figure 23:

## Couche 2 : PPP

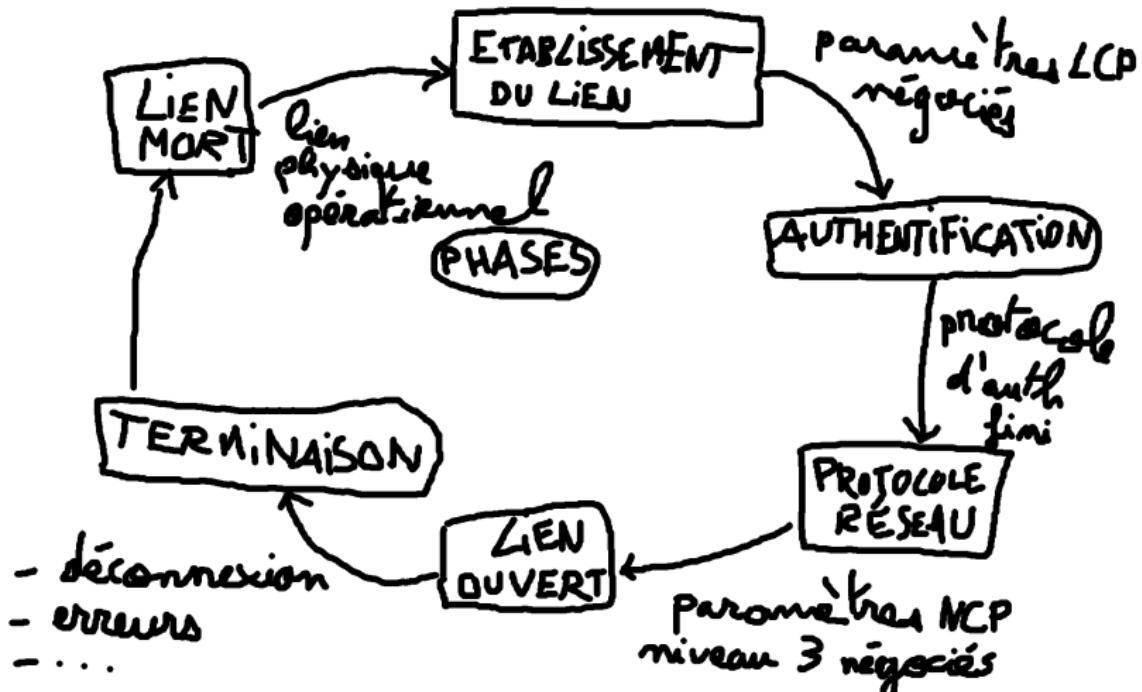


Figure 24:

## Couche 2 : PPP

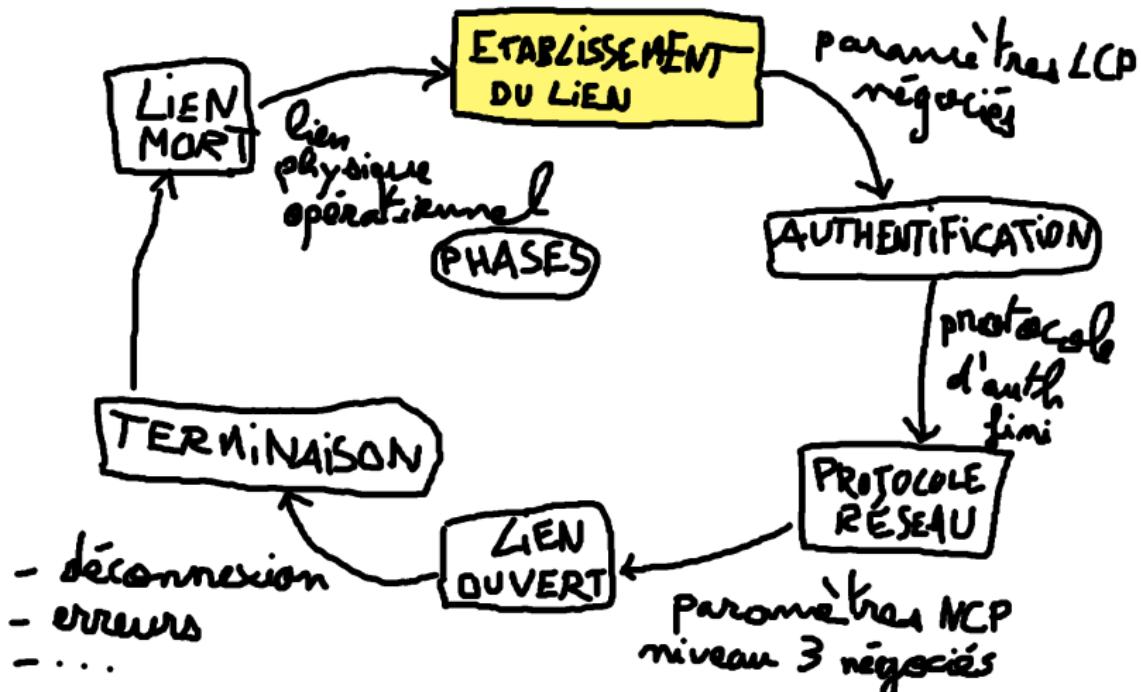


Figure 25:

## Couche 2 : PPP

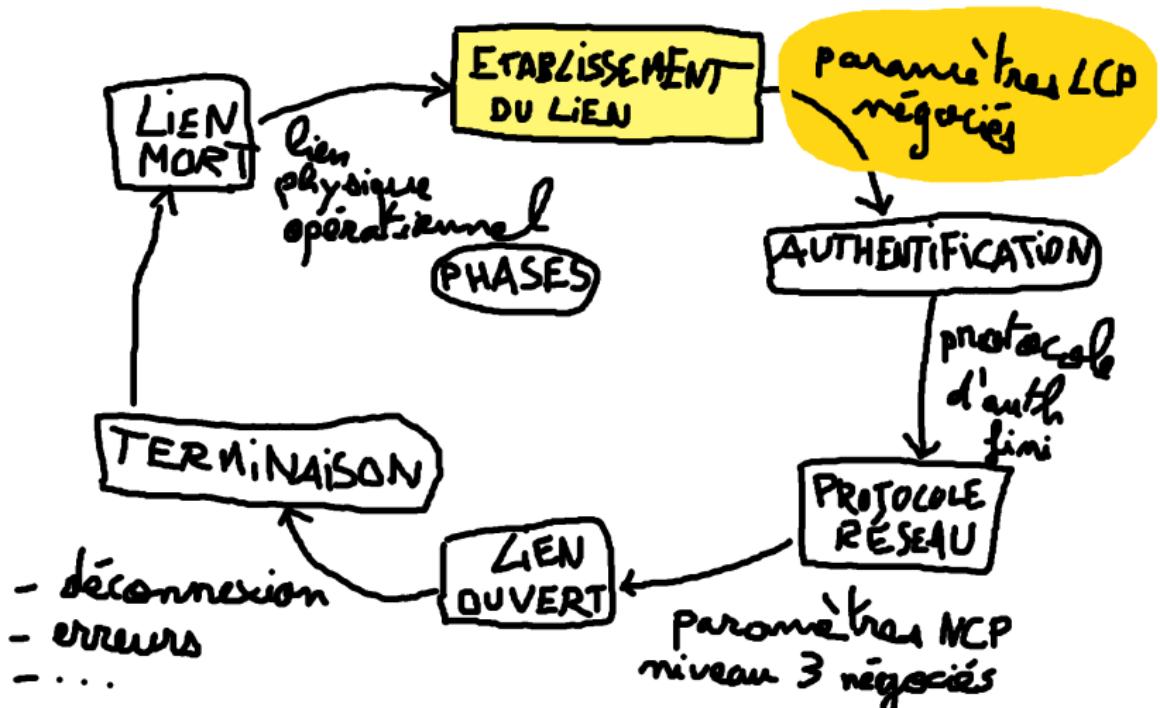


Figure 26:

## Couche 2 : PPP



Figure 27:

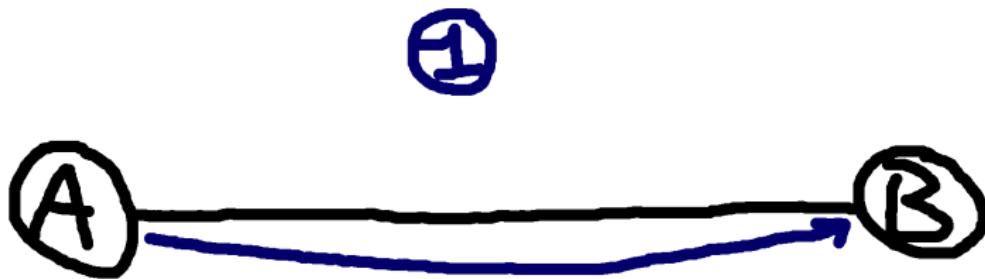
## Couche 2 : PPP

Négociation !



Figure 28:

## Couche 2 : PPP



**Configure-Request avec options :**

- quelle taille de datagramme
- quel protocole d'authentification
- quel protocole de monitoring qualité
- compression des entêtes ?
- ...et autres paramètres

Figure 29:

## Couche 2 : PPP



**Configure-Request avec options :**

- quelle taille de datagramme
- quel protocole d'authentification
- quel protocole de monitoring qualité
- compression des entêtes ?
- ...et autres paramètres

Figure 30:

## Couche 2 : PPP



**Configure-Request avec options :**

- quelle taille de datagramme
- quel protocole d'authentification
- quel protocole de monitoring qualité
- compression des entêtes ?
- ...et autres paramètres

Figure 31:

## Couche 2 : PPP



Configure-Request :

- Cette taille là, alors ?
- Et ce protocole d'auth, peut-être ?
- etc.

Figure 32:

## Couche 2 : PPP

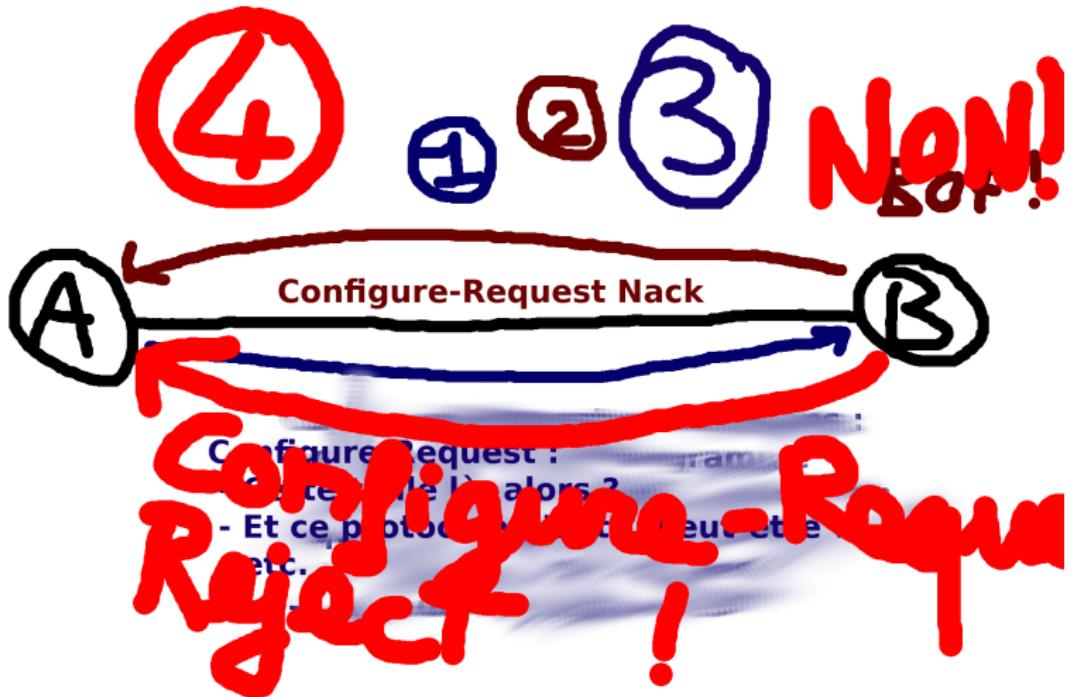


Figure 33:

## Couche 2 : PPP

Phase suivante !

## Couche 2 : PPP

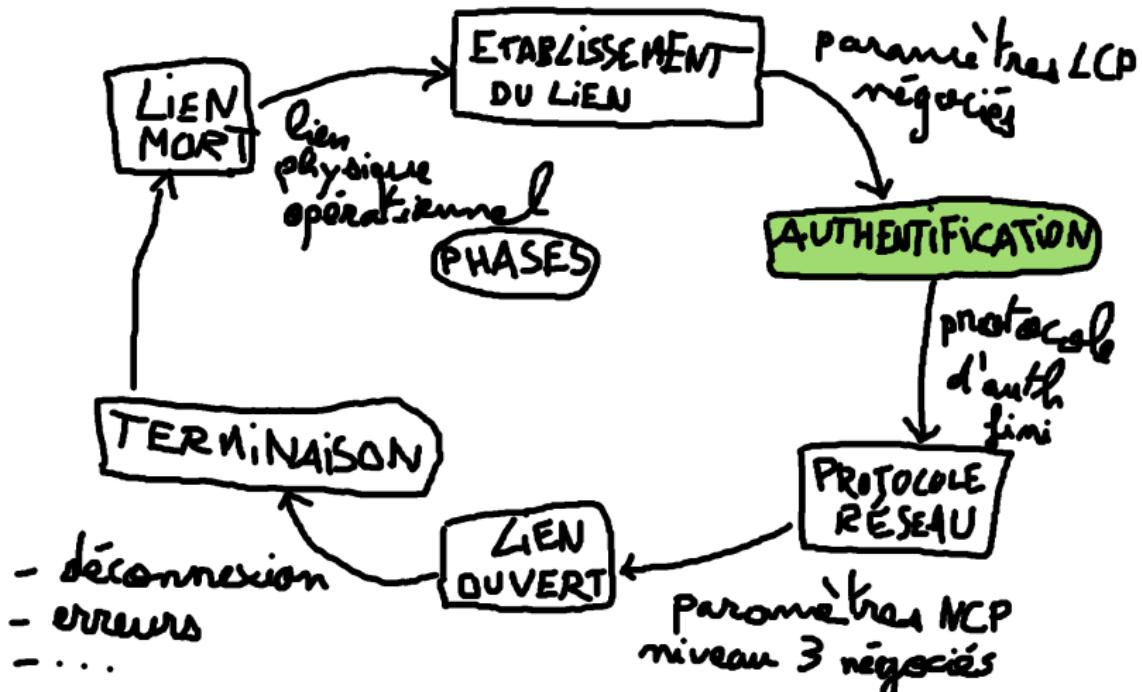


Figure 34:

## Couche 2 : PPP

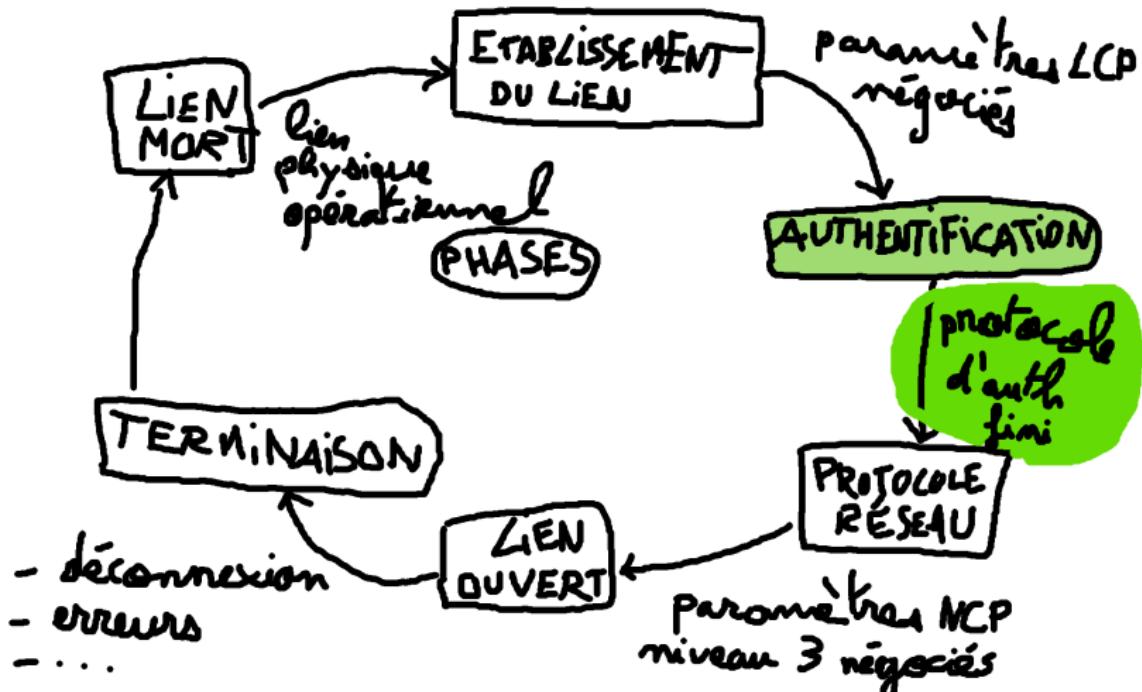


Figure 35:

## Couche 2 : PPP

Premier protocole : **PAP : Password Authentication Protocol**  
Simple...

## Couche 2 : PPP



Figure 36:

# AUTHENTIFICATION!



Figure 37:

## Couche 2 : PPP

PAP *(Password Authentication Protocol)*



Figure 38:

## Couche 2 : PPP

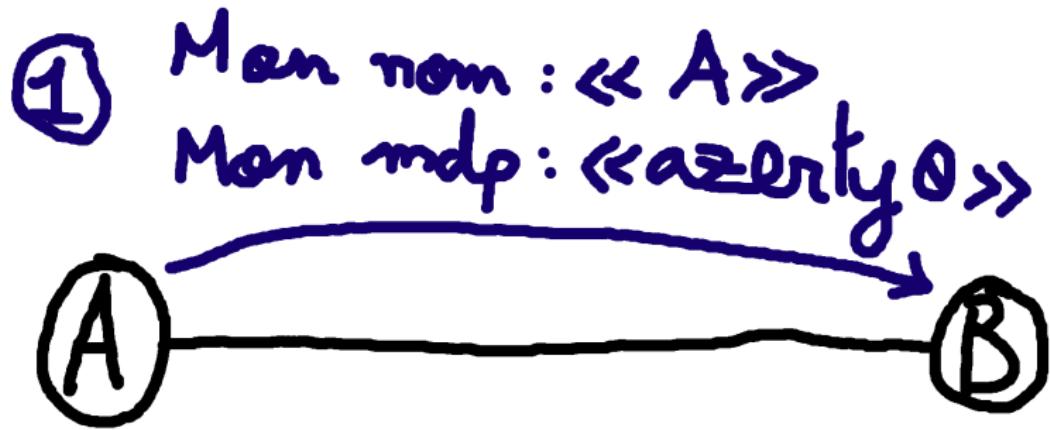
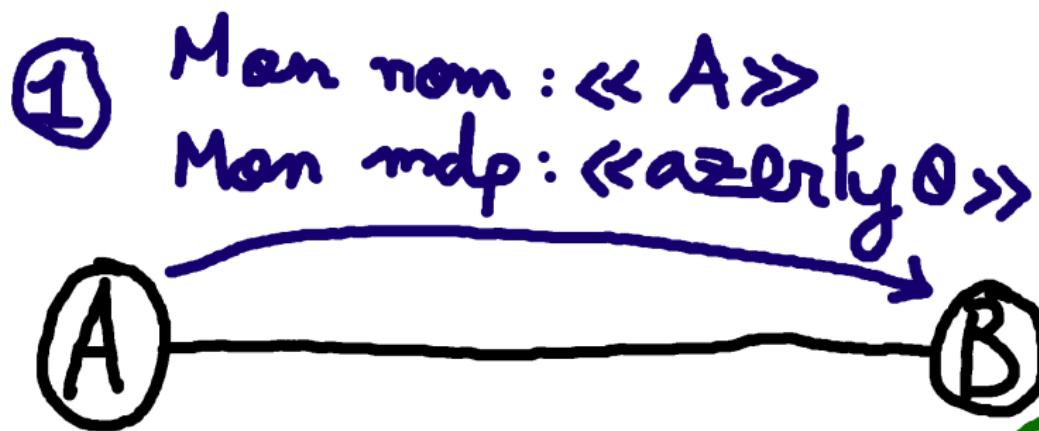


Figure 39:

## Couche 2 : PPP



② regarde  
dans la liste

Figure 40:

## Couche 2 : PPP

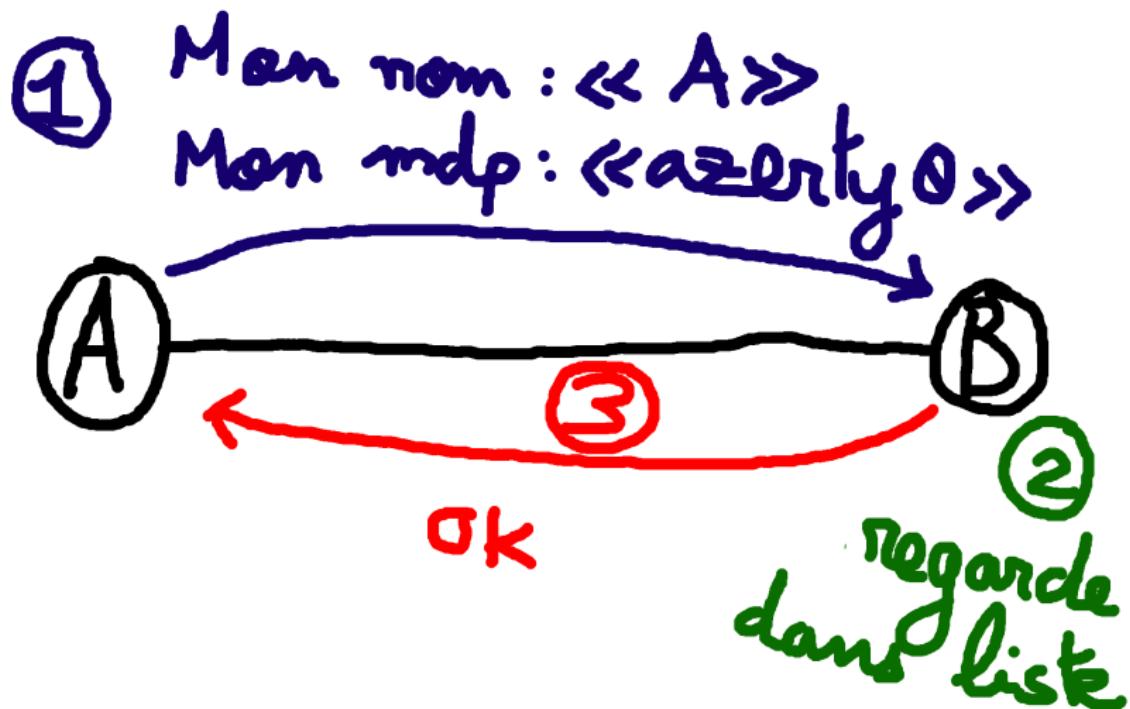


Figure 41:

## Couche 2 : PPP

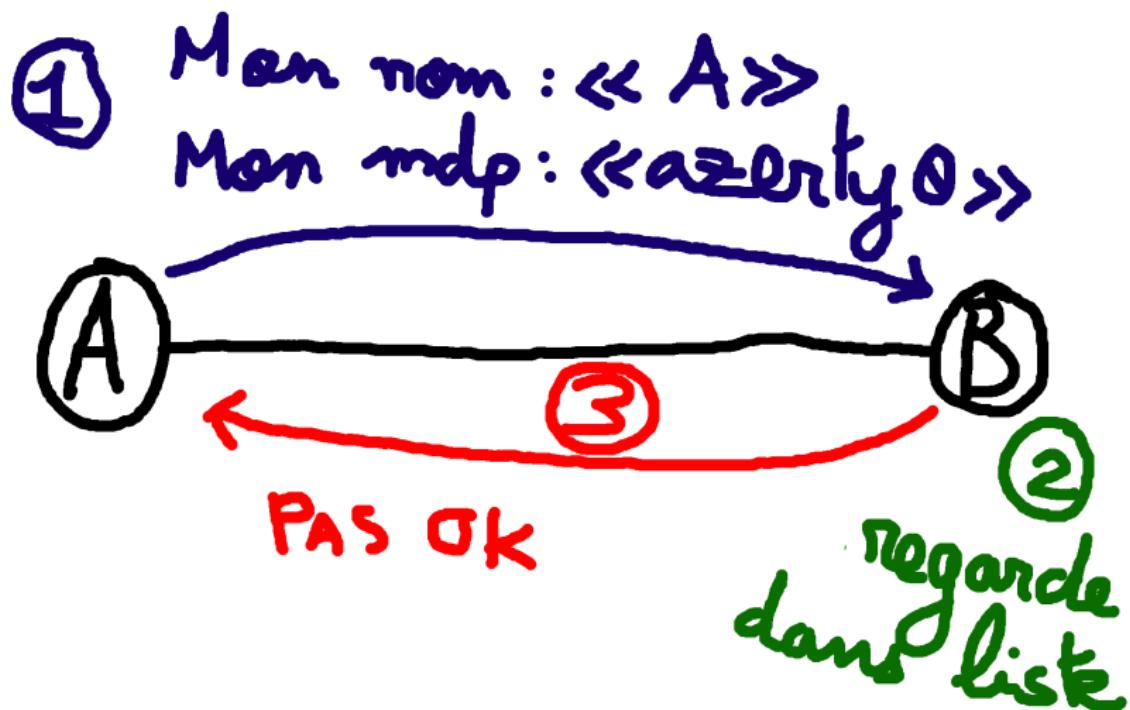


Figure 42:

## Couche 2 : PPP

Que pensez-vous de ce protocole ?

## Couche 2 : PPP

Proposition de meilleur protocole ?

## Couche 2 : PPP

***CHAP : Challenge-Handshake Authentication Protocol***

## Couche 2 : PPP



Figure 43:

# AUTHENTIFICATION!



Figure 44:

## Couche 2 : PPP

**CHAP** (*Challenge-Handshake Authentication Protocol*)



Figure 45:

## Couche 2 : PPP



Figure 46:

## Couche 2 : PPP

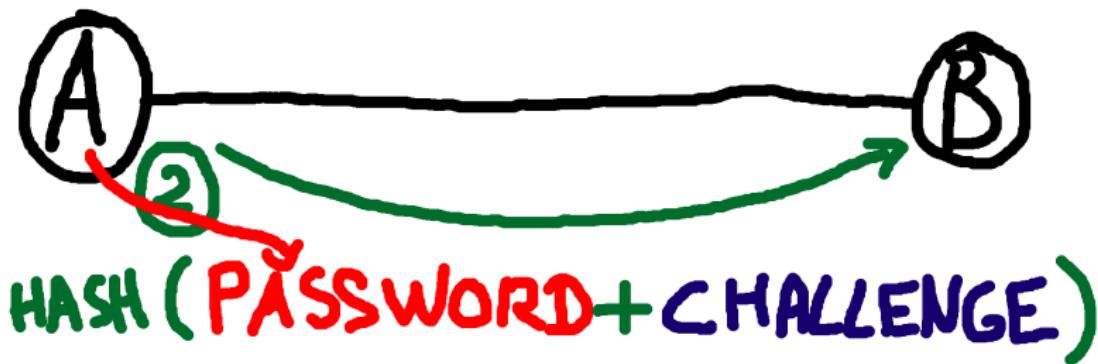


Figure 47:

## Couche 2 : PPP

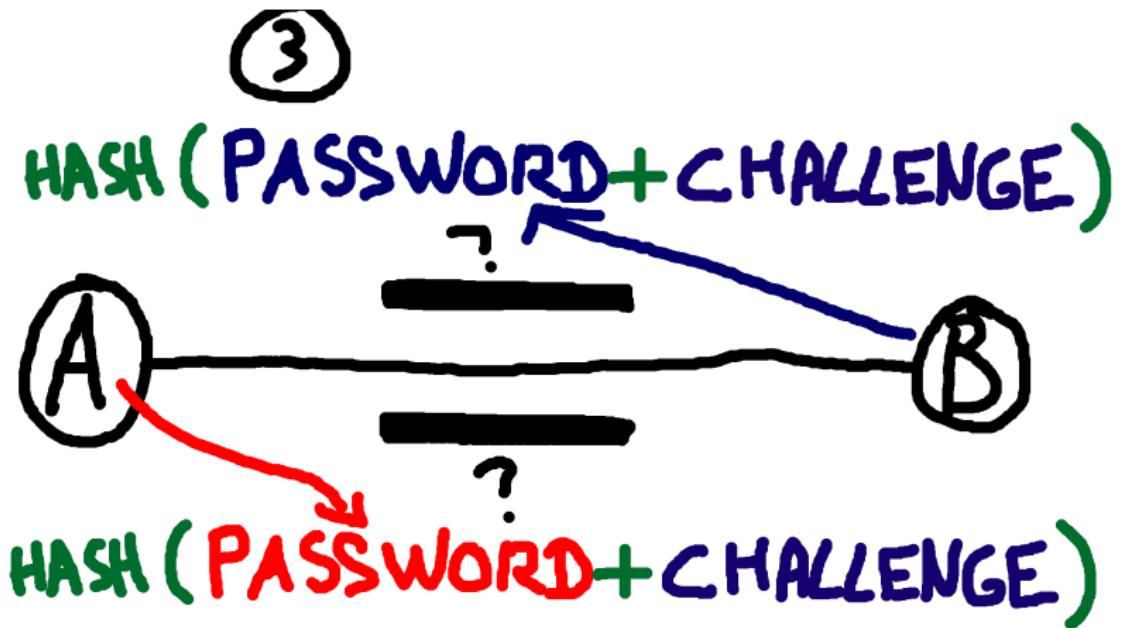


Figure 48:

## Couche 2 : PPP

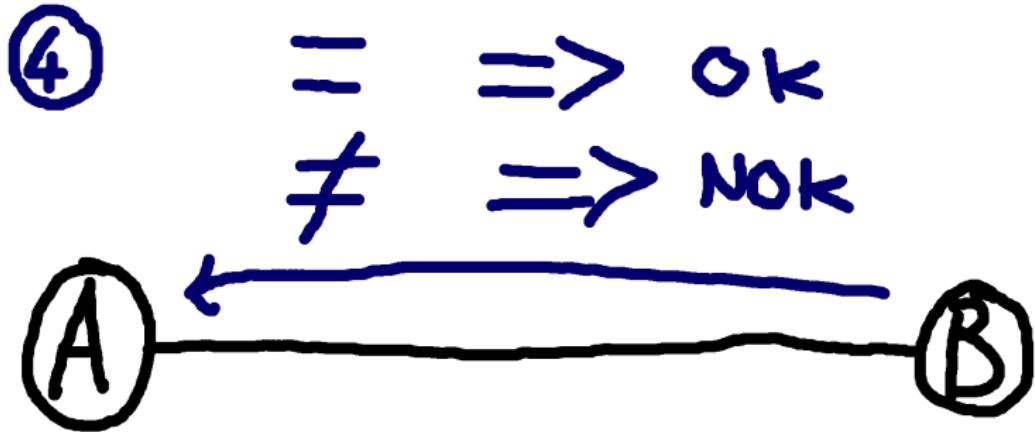


Figure 49:

## Couche 2 : PPP

Phase suivante !

## Couche 2 : PPP

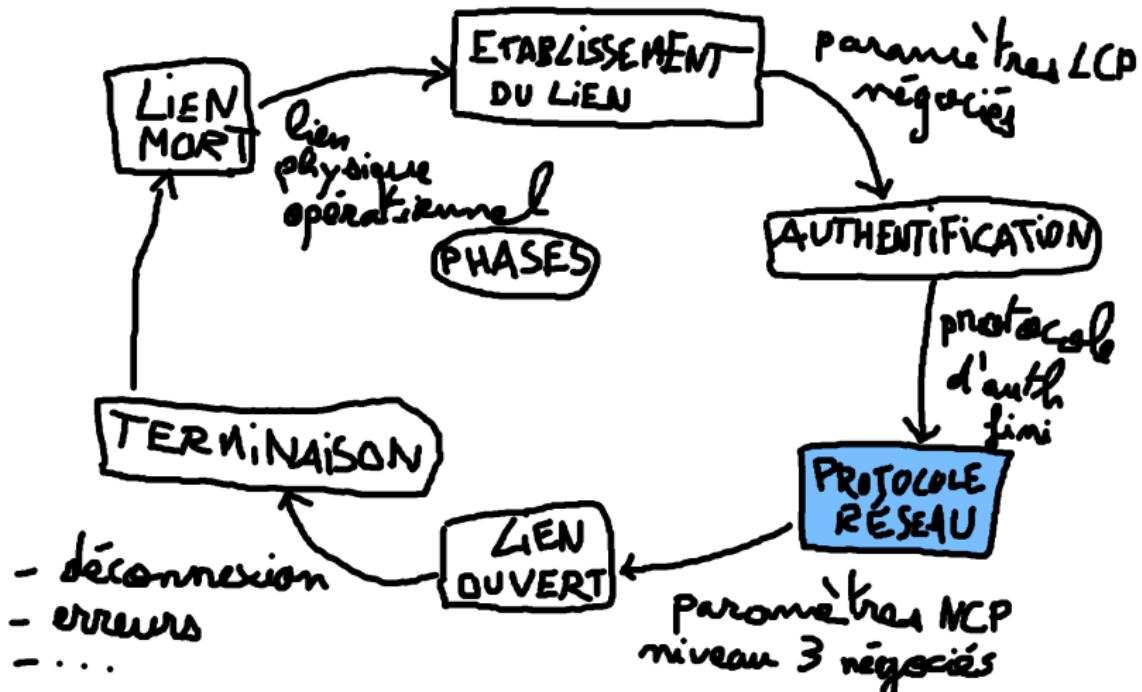


Figure 50:

## Couche 2 : PPP

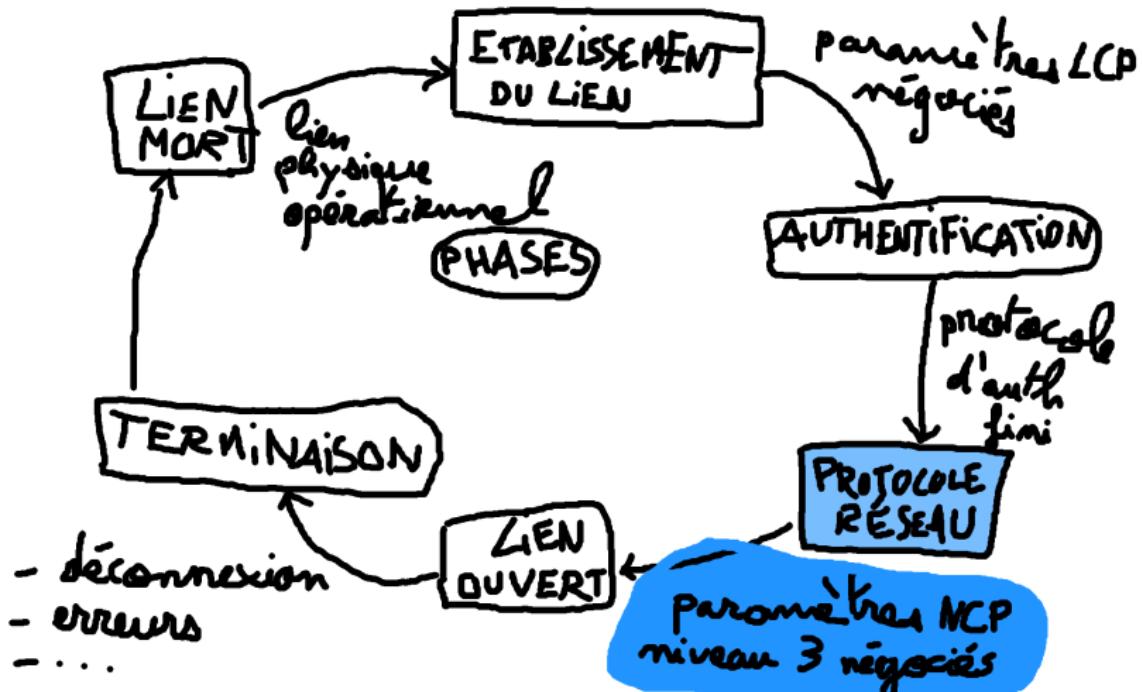


Figure 51:

## Couche 2 : PPP

***NCP = Network Control Protocol***

Configuration de paramètres spécifiques au(x) protocole(s) de couche 3 utilisés.

## Couche 2 : PPP

Cas le plus classique en couche 3 transporté par PPP : IP.  
=> **NCP = IPCP (IP Control Protocol ...)**

## Couche 2 : PPP

À quoi sert **IPCP** ?

- ▶ Négociation de l'utilisation d'entêtes IP réduits ;
- ▶ Obtention d'une adresse IP.

## Couche 2 : PPP

*PPP* a d'autres sous-protocoles :

**LQR** : *Link Quality Reporting*.

## Couche 2 : PPP

*PPP* a d'autres sous-protocoles :

**CCP** : **C**ompression **C**ontrol **P**rotocol.

## Couche 2 : PPP

*PPP* a d'autres sous-protocoles :

**ECP** : **E**nryption **C**ontrol **P**rotocol.

## Couche 2 : PPP

*PPP* a d'autres sous-protocoles :

**MP** : **M**ultilink **P**rotocol.

## Couche 2 : PPP

*PPP* a d'autres sous-protocoles :

**BAP** : *Bandwidth Allocation Protocol*.

**BACP** : *Bandwidth Allocation Control Protocol*.

## Couche 2 : PPP

PPP fait vraiment beaucoup de choses.

## Couche 2 : PPP

Quel format ont les trames PPP ?

Observons la RFC 1662...

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol 8/16 bits	Information *	Padding *
FCS 16/32 bits	Flag 01111110	Inter-frame Fill or next Address

Figure 52:

## Couche 2 : PPP

Flag 01111110	Address	Control
	11111111	00000011
Protocol 8/16 bits	Information *	Padding *
FCS 16/32 bits	Flag 01111110	Inter-frame Fill or next Address

Figure 53:

## Couche 2 : PPP

### Flag Sequence

Each frame begins and ends with a Flag Sequence, which is the binary sequence 01111110 (hexadecimal 0x7e). All implementations continuously check for this flag, which is used for frame synchronization.

## Couche 2 : PPP

Qu'est-ce que ça implique ?

## Couche 2 : PPP

An octet stuffing procedure is used. The Control Escape octet is defined as binary 01111101 (hexadecimal 0x7d), most significant bit first.

As a minimum, sending implementations MUST escape the Flag Sequence and Control Escape octets.

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol	Information	Padding
8/16 bits	*	*
FCS	Flag	Inter-frame Fill
16/32 bits	01111110	or next Address

Figure 54:

## Couche 2 : PPP

### Address Field

The Address field is a single octet, which contains the binary sequence 11111111 (hexadecimal 0xff), the All-Stations address. Individual station addresses are not assigned. The All-Stations address MUST always be recognized and received.

## Couche 2 : PPP

The use of other address lengths and values may be defined at a later time, or by prior agreement. Frames with unrecognized Addresses SHOULD be silently discarded.

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol	Information	Padding
8/16 bits	*	*
FCS	Flag	Inter-frame Fill
16/32 bits	01111110	or next Address

Figure 55:

## Couche 2 : PPP

### Control Field

The Control field is a single octet, which contains the binary sequence 00000011 (hexadecimal 0x03), the Unnumbered Information (UI) command with the the Poll/Final (P/F) bit set to zero.

## Couche 2 : PPP

The use of other Control field values may be defined at a later time, or by prior agreement. Frames with unrecognized Control field values SHOULD be silently discarded.

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol 8/16 bits	Information *	Padding *
FCS 16/32 bits	Flag 01111110	Inter-frame Fill or next Address

Figure 56:

## Couche 2 : PPP

### Protocol Field

The Protocol field is one or two octets, and its value identifies the datagram encapsulated in the Information field of the packet.

The field is transmitted and received most significant octet first.

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol 8/16 bits	Information	Padding *
FCS 16/32 bits	Flag 01111110	Inter-frame Fill or next Address

Figure 57:

## Couche 2 : PPP

### Information Field

The Information field is zero or more octets.

The Information field contains the datagram  
for the protocol specified in the Protocol field.

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol 8/16 bits	Information *	Padding *
FCS 16/32 bits	Flag 01111110	Inter-frame Fill or next Address

Figure 58:

## Couche 2 : PPP

### Padding

On transmission, the Information field MAY be padded with an arbitrary number of octets up to the MRU. It is the responsibility of each protocol to distinguish padding octets from real information.

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol 8/16 bits	Information *	Padding *
FCS 16/32 bits	Flag 01111110	Inter-frame Fill or next Address

Figure 59:

## Couche 2 : PPP

Frame Check Sequence (FCS) Field

## Couche 2 : PPP

Flag	Address	Control
01111110	11111111	00000011
Protocol 8/16 bits	Information *	Padding *
FCS 16/32 bits	Flag 01111110	Inter-frame Fill or next Address

Figure 60:

## Couche 2 : PPP

En pratique...

## Couche 2 : PPP

 informations système - FTTH  aide

Cette page vous permet de consulter différentes informations de la Livebox.

**Livebox-**

2.1 statut du lien FTTH	 connecté	 imprimer
2.2 MAC adresse du WAN		
2.3 état de la connexion	 synchronisé	
2.6 statut de connexion PPP	 connecté	
2.7 statut du compte	disponible	
2.8 nom de compte Internet		
2.9 mode d'authentification PPP	CHAP	
2.10 dernière connexion PPP	23 avril, 16:32:54	
2.11 durée de connexion PPP	2 jours, 19:47:47	
2.12 type de protocole PPP	PPPoE	
2.13 dernière erreur de connexion PPP	aucune erreur	
2.14 date de dernière déconnexion PPP	23 avril, 16:32:48	
2.15 VLAN ID/PRI	835/0	

Figure 61:

## Couche 2 : PPP

 informations système - FTTH  aide

Cette page vous permet de consulter différentes informations de la Livebox.

Livebox-

2.1 statut du lien FTTH	 connecté
2.2 MAC adresse du WAN	
2.3 état de la connexion	 synchronisé
2.6 statut de connexion PPP	 connecté
2.7 statut du compte	disponible
2.8 nom de compte Internet	
2.9 mode d'authentification PPP	 CHAP
2.10 dernière connexion PPP	23 avril, 16:32:54
2.11 durée de connexion PPP	2 jours, 19:47:47
2.12 type de protocole PPP	 PPPoE
2.13 dernière erreur de connexion PPP	aucune erreur
2.14 date de dernière déconnexion PPP	23 avril, 16:32:48
2.15 VLAN ID/PRI	835/0

 imprimer

Figure 62:

Retour à la couche physique : réseaux sans fil

## Réseaux sans fil

Dans un réseau sans fil, il n'y a pas de fil entre les stations.

# Réseaux sans fil

Comment peuvent-elles communiquer ?

- ▶ Ondes électromagnétiques ;
- ▶ Ondes “sonores” ;

## Réseaux sans fil



Figure 63: saint-bernard

## Réseaux sans fil

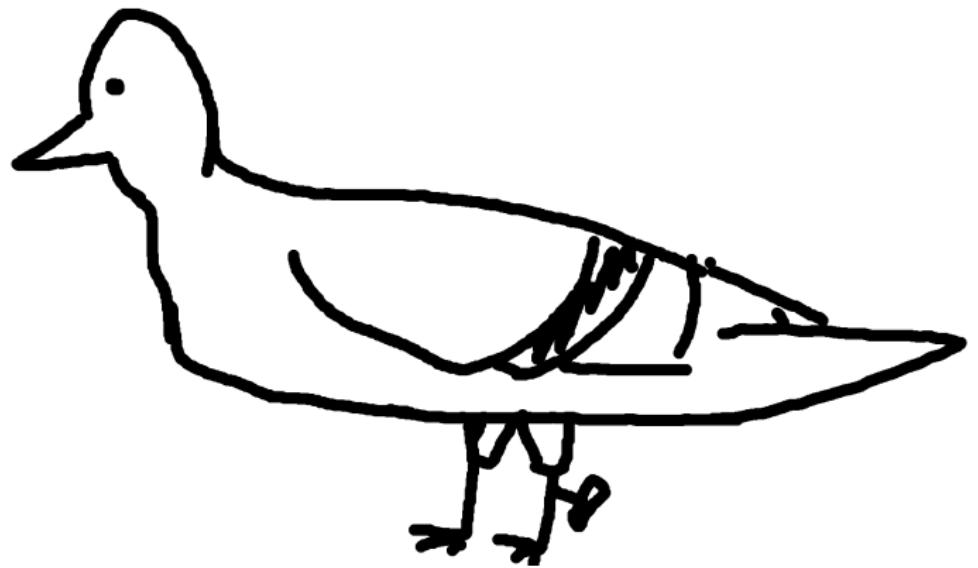


Figure 64: RFC1149

## Réseaux sans fil

Mais généralement, ondes radio.

# Réseaux sans fil

Désignation internationale	Désignation francophone	Fréquence	Longueur d'onde	Autres appellations	Exemples d'utilisation
ELF ( <i>extremely low frequency</i> )	EBF (extrêmement basse fréquence)	3 Hz à 30 Hz	100 000 km à 10 000 km		Détection de phénomènes naturels
SLF ( <i>super low frequency</i> )	SBF (super basse fréquence)	30 Hz à 300 Hz	10 000 km à 1 000 km		Communication avec les sous-marins
ULF ( <i>ultra low frequency</i> )	UBF (ultra basse fréquence)	300 Hz à 3 000 Hz	1 000 km à 100 km		Détection de phénomènes naturels
VLF ( <i>very low frequency</i> )	TBF (très basse fréquence)	3 kHz à 30 kHz	100 km à 10 km	ondes myriamétriques	Communication avec les sous-marins, Implants médicaux, Recherches scientifiques...
LF ( <i>low frequency</i> )	BF (basse fréquence)	30 kHz à 300 kHz	10 km à 1 km	grandes ondes ou ondes longues ou kilométriques	Radioamateur, Radionavigation, Radiodiffusion GO, Radio-identification
MF ( <i>medium frequency</i> )	MF (moyenne fréquence)	300 kHz à 3 MHz	1 km à 100 m	petites ondes ou ondes moyennes ou hectométriques	Radioamateur, Radio AM, Service maritime, Appareil de recherche de victimes d'avalanche
HF ( <i>high frequency</i> )	HF (haute fréquence)	3 MHz à 30 MHz	100 m à 10 m	ondes courtes ou décamétriques	Organisations diverses, Militaire, Radiodiffusion, Maritime, Aéronautique, Radioamateur, Météo, Radio de catastrophe, etc.

Figure 65: [https://fr.wikipedia.org/wiki/Onde\\_radio](https://fr.wikipedia.org/wiki/Onde_radio)

# Réseaux sans fil

VHF ( <i>very high frequency</i> )	THF (très haute fréquence)	30 MHz à 300 MHz	10 m à 1 m	ondes ultra-courtes ou métriques	Radio FM, Aéronautique, Maritime, Radioamateur, Gendarmerie nationale française, Pompiers, SAMU, Réseaux privés, taxis, militaire, Météo, etc.
UHF ( <i>ultra high frequency</i> )	UHF (ultra haute fréquence)	300 MHz à 3 GHz	1 m à 10 cm	ondes décimétriques	Réseaux privés, militaire, GSM, GPS, téléphones sans fil (DECT), Wi-Fi, Télévision, Radioamateur, etc.
SHF ( <i>super high frequency</i> )	SHF (super haute fréquence)	3 GHz à 30 GHz	10 cm à 1 cm	ondes centimétriques	Réseaux privés, Wi-Fi, Micro-onde, Radiodiffusion par satellite (TV), Faisceau hertzien, Radar météorologique, Radioamateur, etc.
EHF ( <i>extremely high frequency</i> )	EHF (extrêmement haute fréquence)	30 GHz à 300 GHz	1 cm à 1 mm	ondes millimétriques	Réseaux privés, Radars anticollision pour automobiles, Liaisons vidéo transportables, Faisceau hertzien, Radioamateur, etc.
Térahertz	Térahertz	300 GHz à 3 000 GHz	1 mm à 100 µm	ondes submillimétriques	

Figure 66: [https://fr.wikipedia.org/wiki/Onde\\_radio](https://fr.wikipedia.org/wiki/Onde_radio)

# Réseaux sans fil

En bref :

1. Les ondes radio sont des ondes électromagnétiques
2. Plus la fréquence est haute, plus le signal est atténué (plus de "choses" deviennent des obstacles) ;
3. Fréquence (temporelle) et longueur d'onde (spatiale) sont liées ;
4. Différentes bandes de fréquences ont différents usages.

## Réseaux sans fil

Pour transmettre le signal, il faut une antenne.

## Réseaux sans fil

Antenne basique : antenne dipolaire.

## Réseaux sans fil

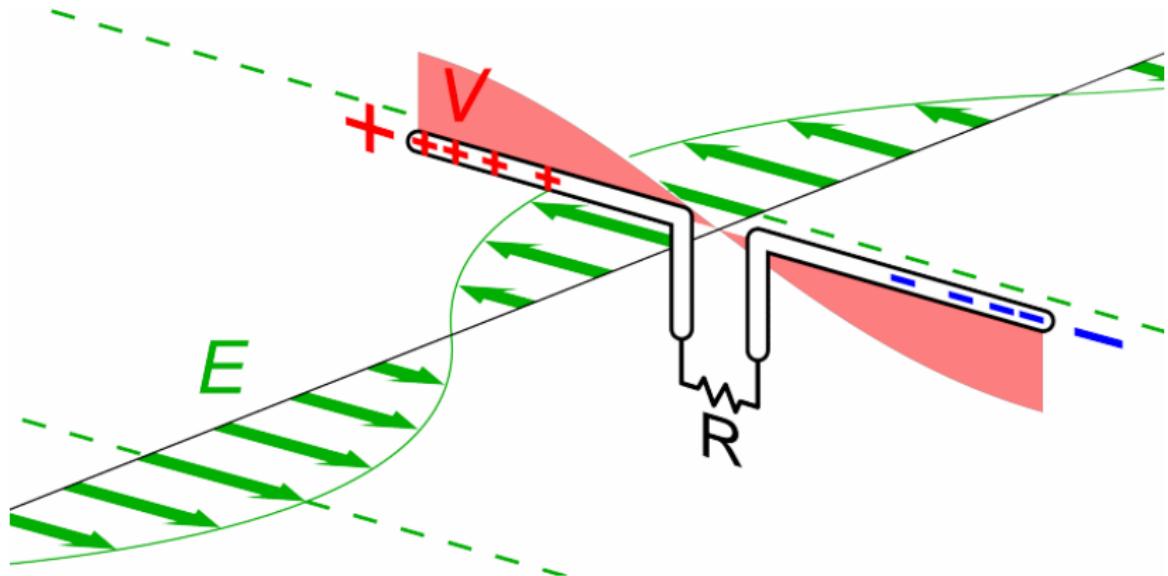


Figure 67: [https://fr.wikipedia.org/wiki/Antenne\\_dipolaire](https://fr.wikipedia.org/wiki/Antenne_dipolaire)

## Réseaux sans fil

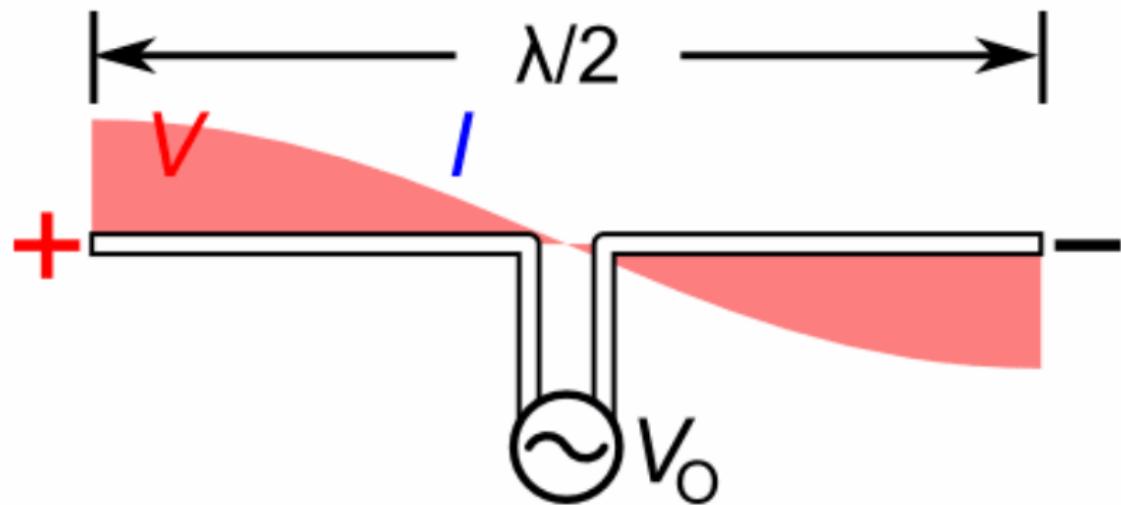


Figure 68: [https://fr.wikipedia.org/wiki/Antenne\\_dipolaire](https://fr.wikipedia.org/wiki/Antenne_dipolaire)

## Réseaux sans fil

Taille de l'antenne liée à la longueur d'onde qu'on veut transmettre.  
Bonne taille, souvent :  $L / 2$ .

## Réseaux sans fil

La caractéristique essentielle d'une antenne est :

***Dans quelle direction rayonne-t-elle ?***

## Réseaux sans fil

Antenne ***isotropique***. Théorique.

Rayonne dans toutes les directions avec la même puissance.

## Réseaux sans fil

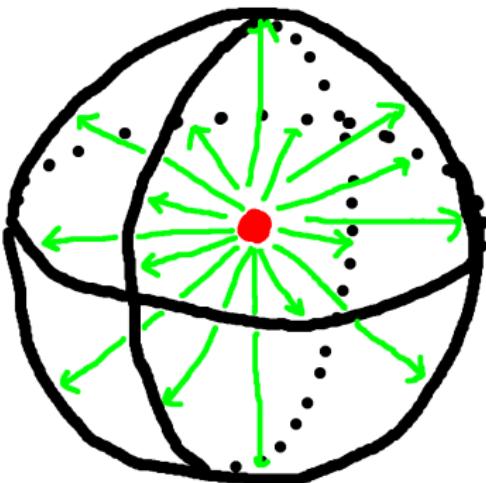


Figure 69: diagramme rayonnement antenne isotropique (théorique)

## Réseaux sans fil



Figure 70: antenne dipolaire

## Réseaux sans fil

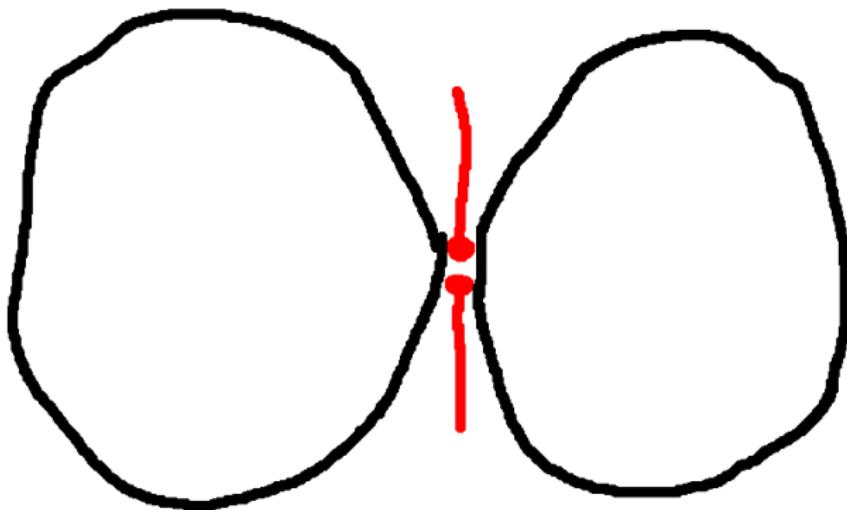


Figure 71: diagramme rayonnement 2D antenne dipolaire

## Réseaux sans fil

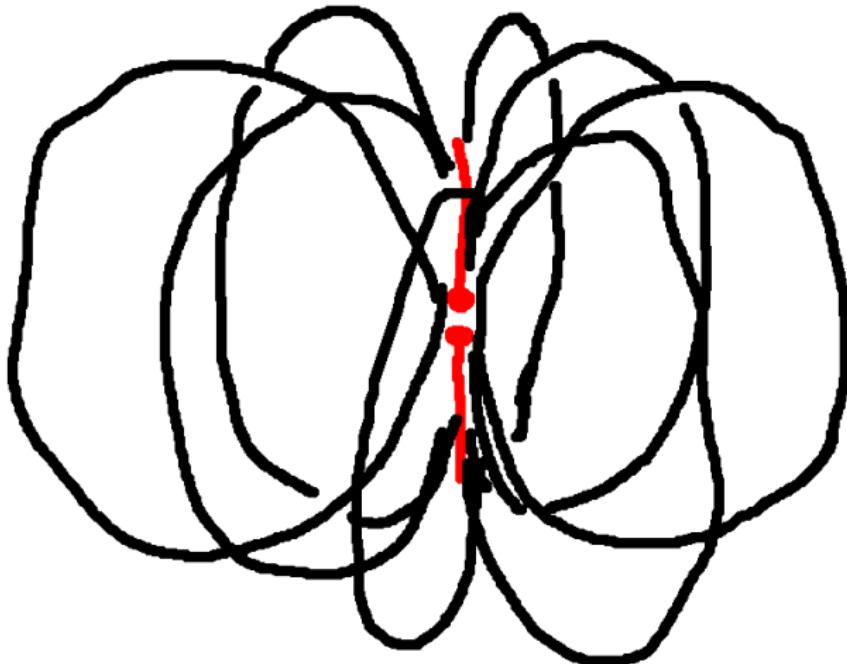


Figure 72: diagramme rayonnement 3D antenne dipolaire

## Réseaux sans fil

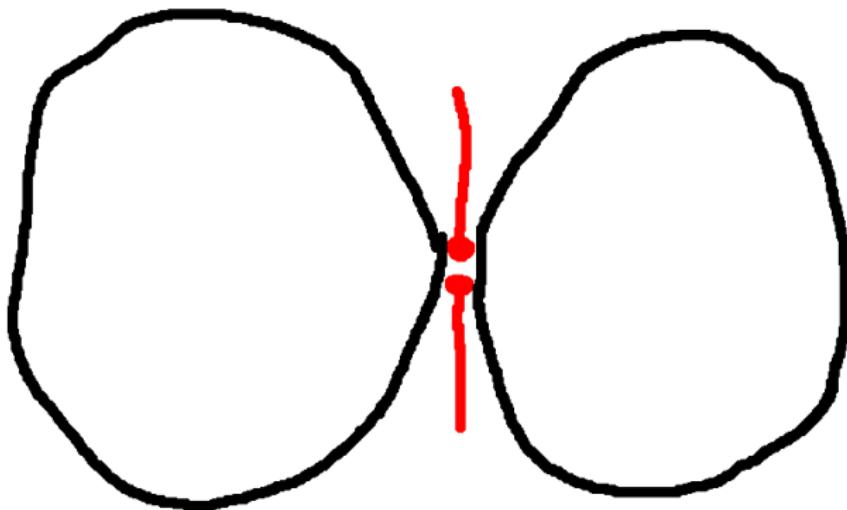


Figure 73: diagramme rayonnement 2D antenne dipolaire

## Réseaux sans fil

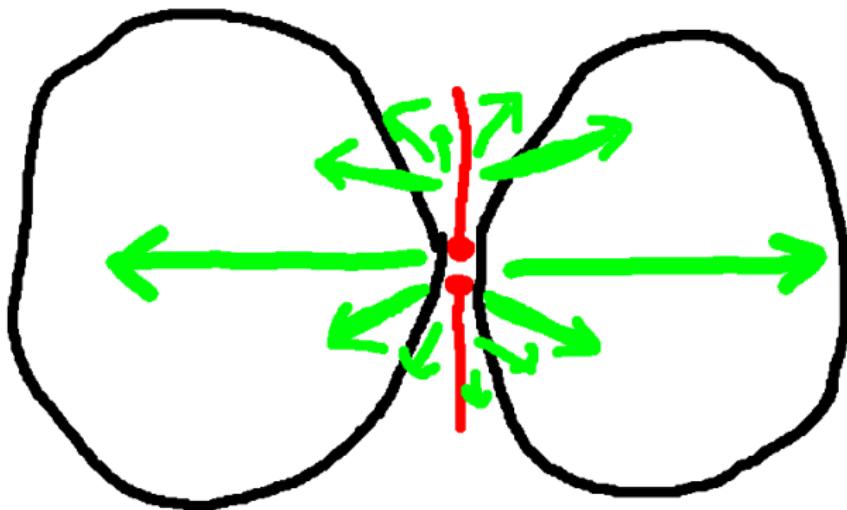


Figure 74: diagramme rayonnement 2D antenne dipolaire

## Réseaux sans fil

Gain d'antenne =

*Le gain d'antenne est le pouvoir d'amplification passif d'une antenne. C'est le rapport entre la puissance rayonnée dans le lobe principal et la puissance rayonnée par une antenne de référence, isotrope ou dipolaire. Le gain d'une antenne dépend principalement de sa surface équivalente, de sa directivité et de la fréquence.*  
*([https://fr.wikipedia.org/wiki/Gain\\_d'antenne](https://fr.wikipedia.org/wiki/Gain_d'antenne))*

## Réseaux sans fil

- ▶ Donc plus une antenne est *directive*, plus son gain est élevé.
- ▶ On mesure le gain en *dBi* (décibel *isotrope*, parce qu'on compare à une antenne isotrope)

## Réseaux sans fil

Comment augmenter fortement le gain ? Une idée ?

## Réseaux sans fil



Figure 75: p

## Réseaux sans fil

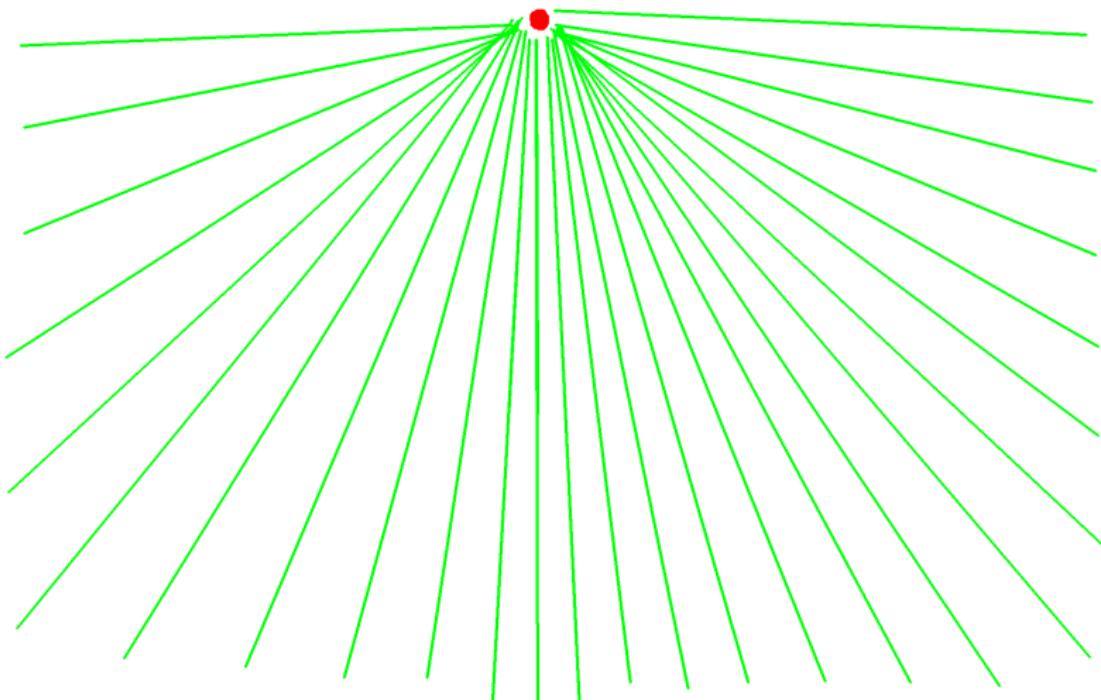


Figure 76: a

## Réseaux sans fil

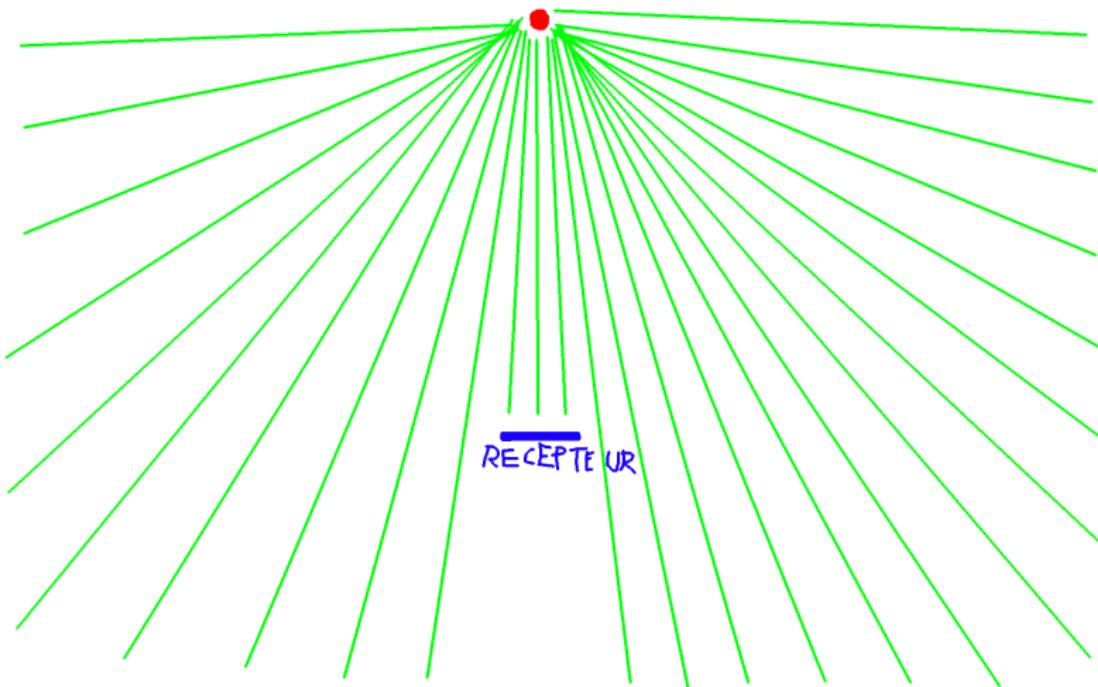


Figure 77: r

## Réseaux sans fil

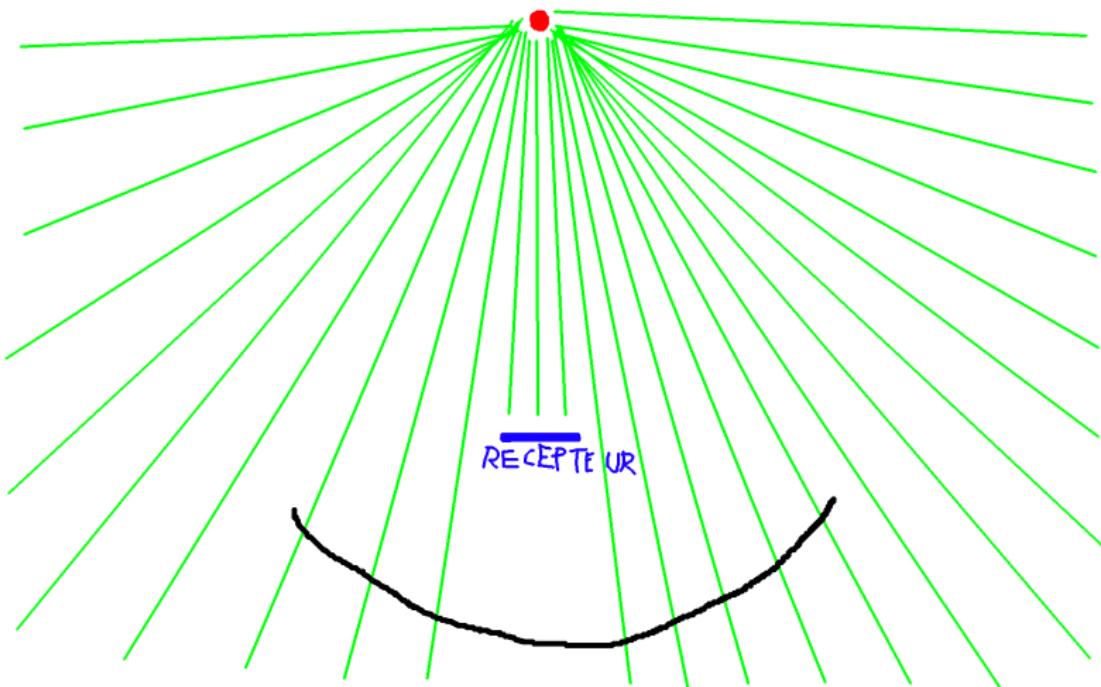


Figure 78: a

## Réseaux sans fil

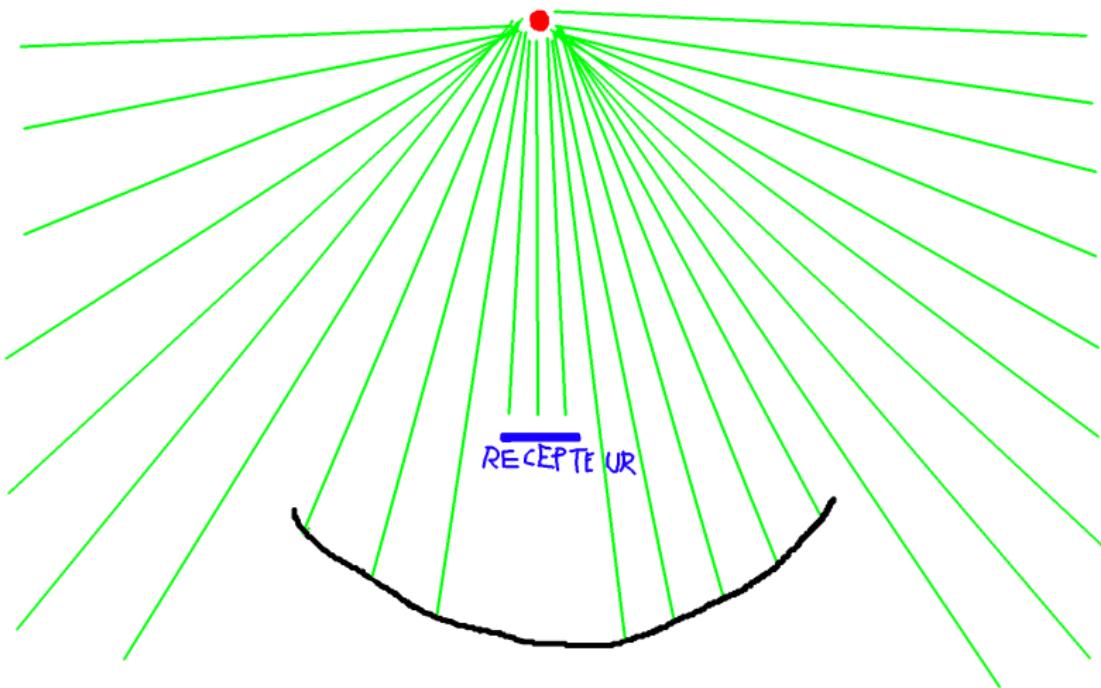


Figure 79: b

## Réseaux sans fil

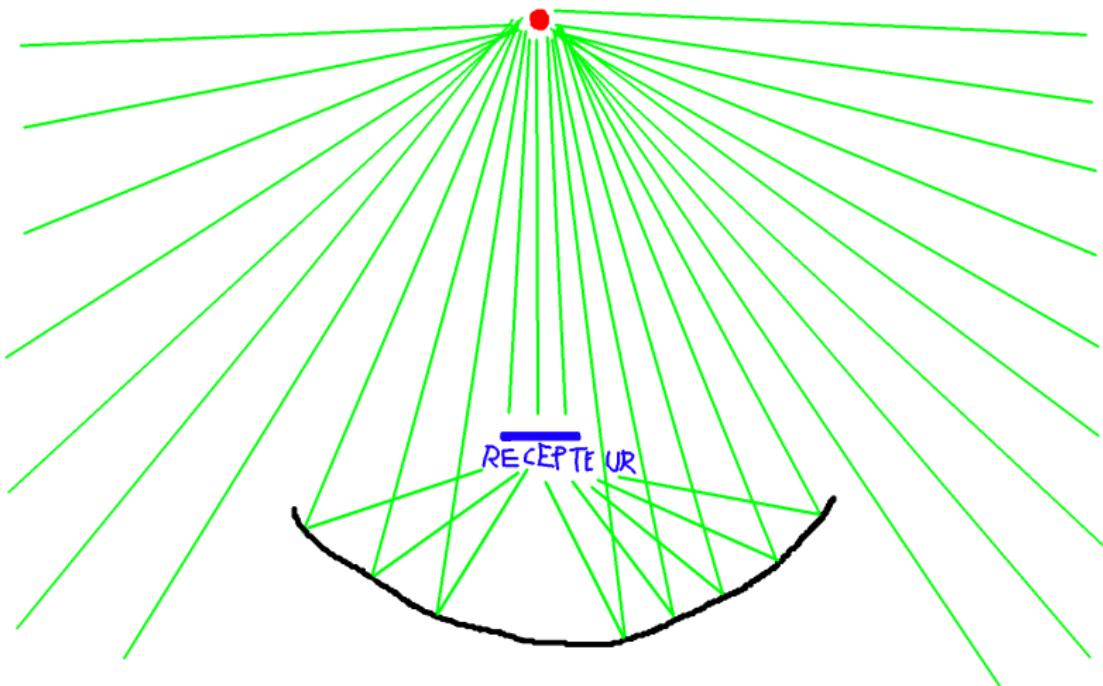


Figure 80: parabole

## Réseaux sans fil

Il y a beaucoup de formes d'antennes, chacune avec son gain. . .

## Réseaux sans fil



Figure 81:

# Réseaux sans fil

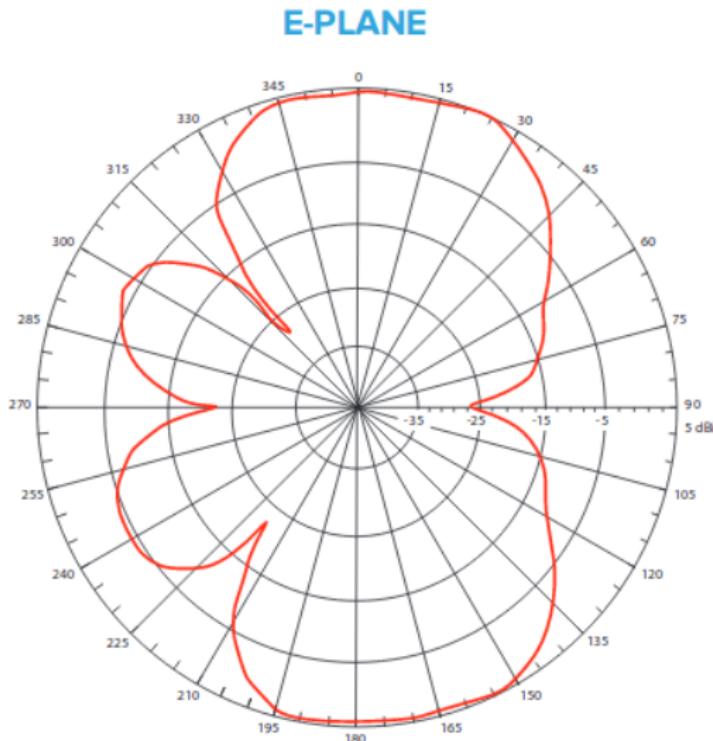


Figure 82: datasheet antenne longue

# Réseaux sans fil

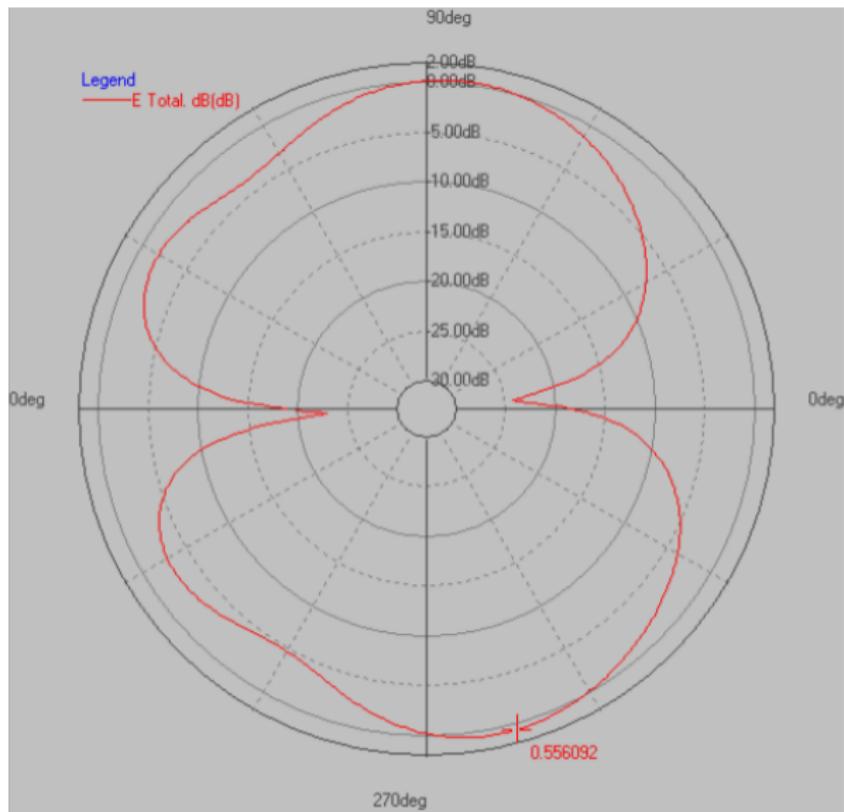


Figure 83: datasheet antenne courte

## Réseaux sans fil

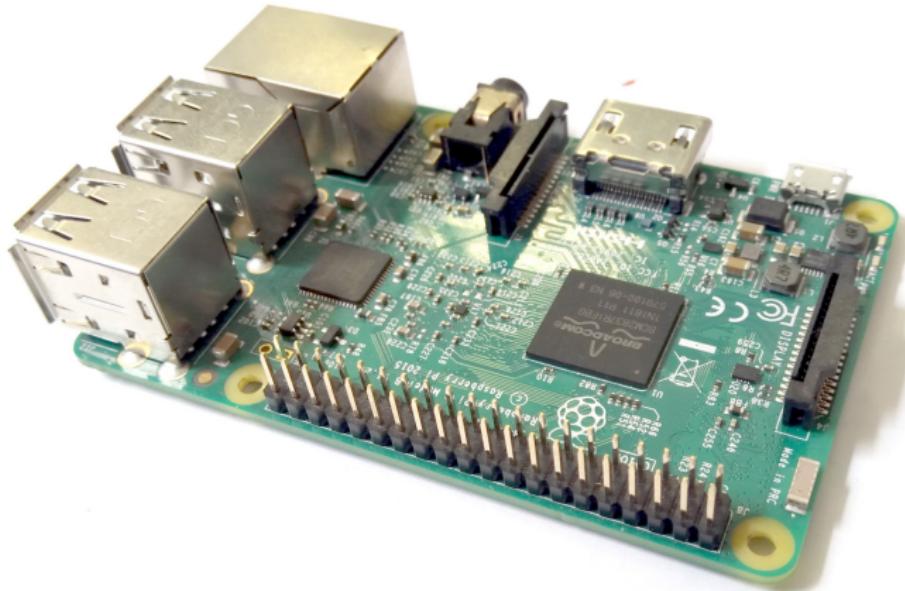


Figure 84: Raspberry Pi 3 : où est l'antenne ?

## Réseaux sans fil

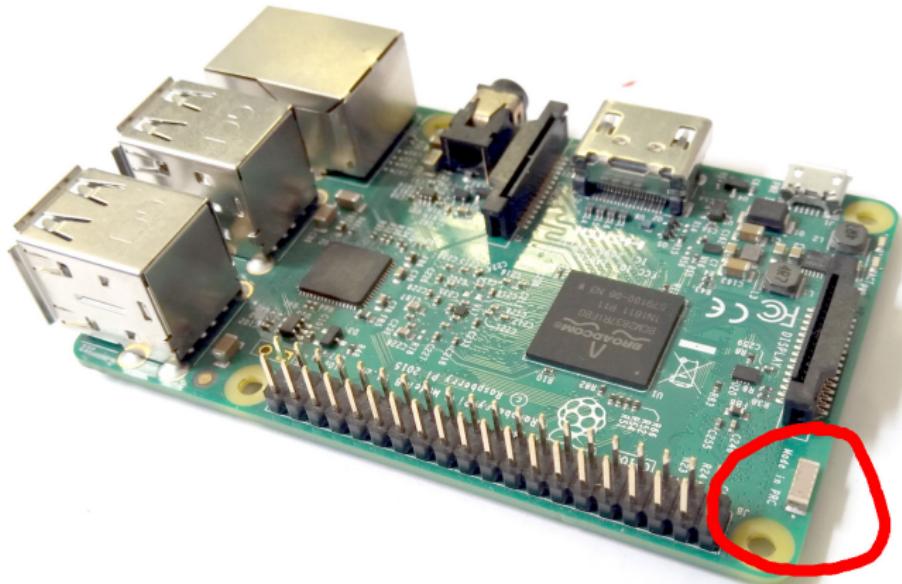


Figure 85: Raspberry Pi 3 : là

## Réseaux sans fil

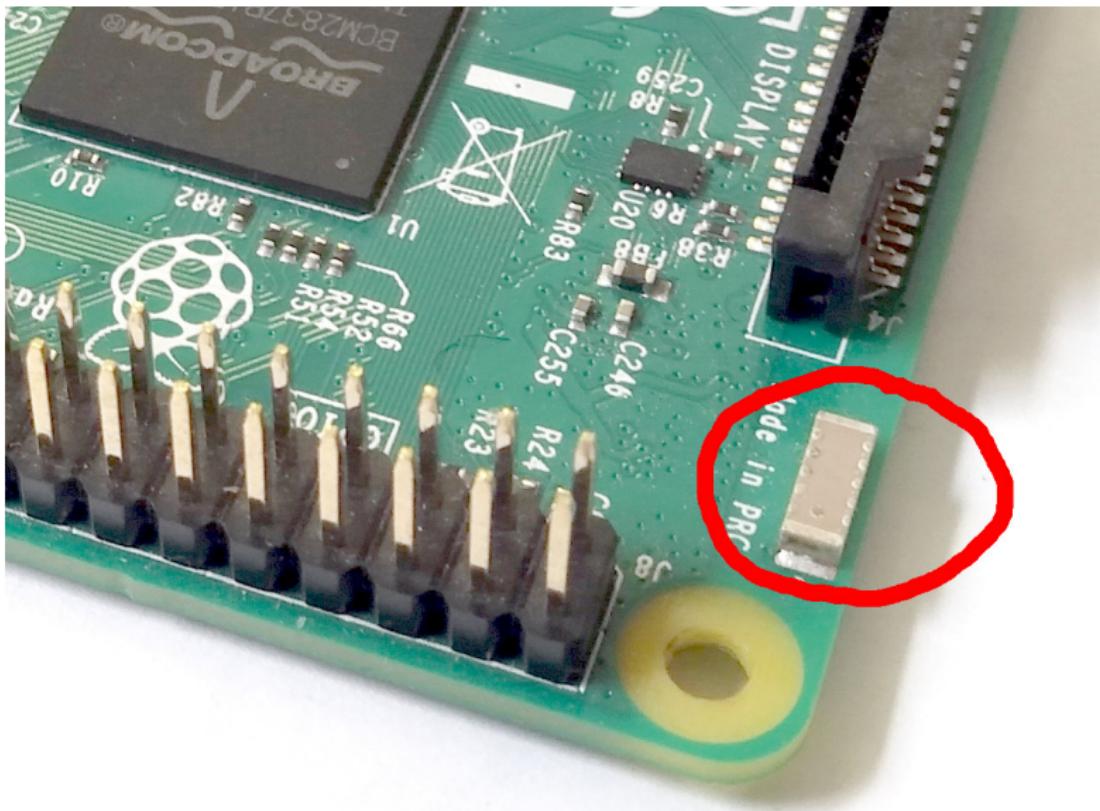


Figure 86: Raspberry Pi 3 : ici

## Réseaux sans fil

Une plus grosse antenne maintenant :

- ▶ 860-870 MHz (LoRa : 868 MHz)
- ▶ 360 degrés à l'horizontale, 25 degrés à la verticale
- ▶ 6 dBi
- ▶ 50W

## Réseaux sans fil



Figure 87: Antenne 868 MHz

## Réseaux sans fil

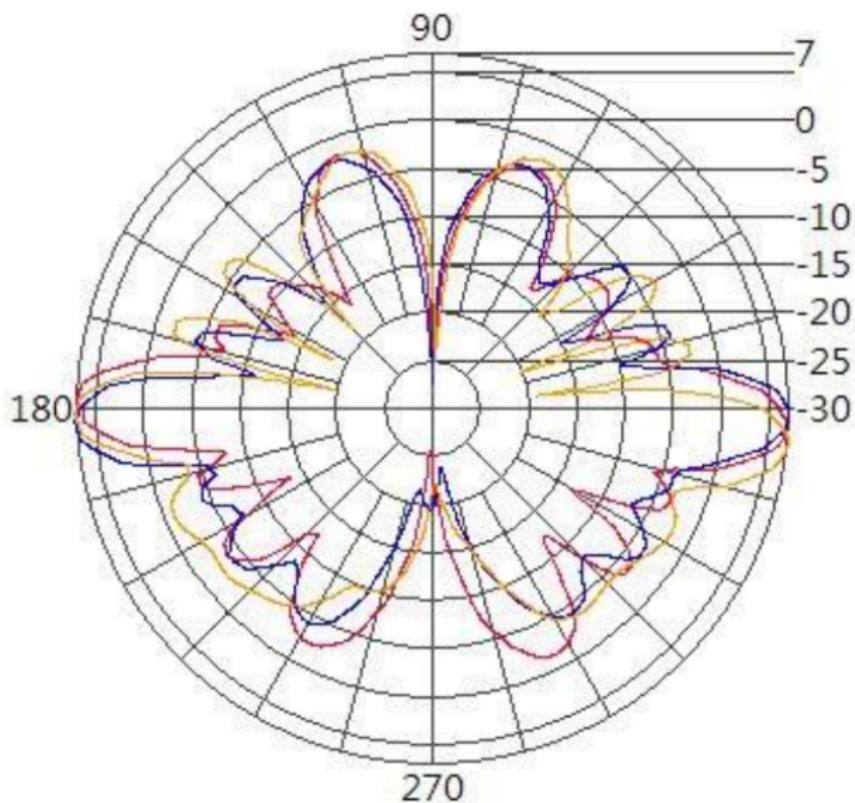


Figure 88: Antenne 868 MHz

## Réseaux sans fil

Attention : une antenne est influencée par ce qu'il y a autour.

- ▶ cf. parabole...
- ▶ cf. intérieur téléphone portable