

# Informatique Industrielle



Support de cours  
Informatique Industrielle  
Module Réseaux : M3103  
Semestre 3

Ce ..... est à compléter !

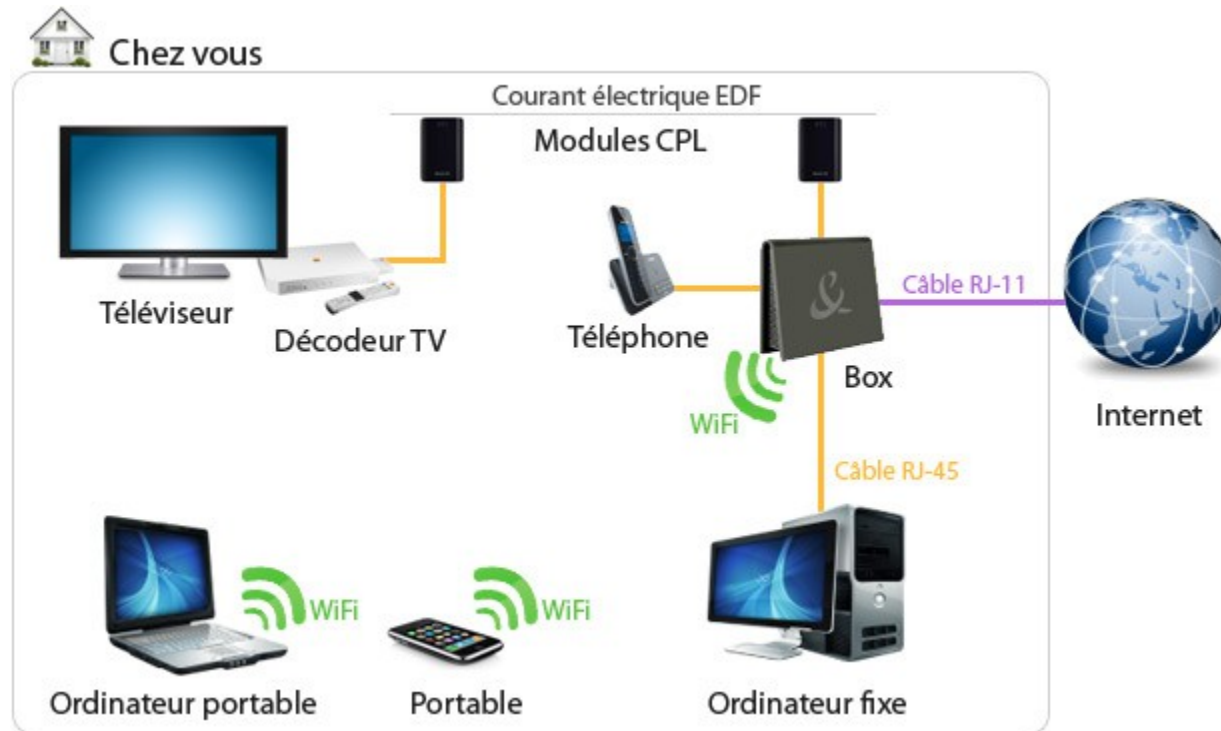
## Extrait du PPN

Référence du module <b>M 3103 (Res3)</b>	Module <b>Réseaux</b>	Semestre <b>S3</b>
<b>Objectifs du module :</b> A partir du cahier des charges, être en mesure de mettre en œuvre, installer, configurer, diagnostiquer un réseau de communication. Comprendre les méthodes et techniques générales de transmission de données employées dans les réseaux de communication, dans le cadre d'une modélisation générale des réseaux de communication à vocation industrielle : automatisme, domotique, immotique. Comprendre les concepts des réseaux industriels de communication et appréhender une classification des réseaux afin de pouvoir réaliser le choix d'un réseau en fonction de spécifications techniques du besoin. Savoir utiliser Ethernet comme solution de communication industrielle, en local ou à distance (TCP/IP). Comprendre les spécificités des implémentations industrielles d'Ethernet.		
<b>Compétences visées :</b> Participer à la mise en œuvre des réseaux reliant des équipements hétérogènes dans le monde industriel. Utiliser les protocoles d'application généralistes utilisés dans le monde Internet. Configurer et exploiter un équipement informatique industriel ou de bureau en réseau exploitant les protocoles d'interconnexion TCP/IP. Exploiter les protocoles pour le contrôle commande de processus par Internet.		
<b>Mots clés :</b> Réseaux, support physique, normalisation, modèle OSI, Ethernet, Internet.		

# I/ Généralités

## I.1/ Définition

C'est un ensemble de systèmes informatisés connectés entre eux dans le but d'échanger des informations.



## I.2/ Objectif des réseaux

Un réseau informatique sert à s'affranchir des distances, il permet:

- Le partage de ressources physiques: espace disque, imprimante...
- Le partage de données ou de programmes...
- D'assurer le rôle d'un média de communication: mail, forum de news, WEB, jeux...
- ...

## I.3/ Les différents types de réseaux (caractérisation suivant la taille)

### •LAN:

Les réseaux LAN (local area network) sont les réseaux locaux. Ils sont étendus à l'échelle d'une salle ou un bâtiment.

Ex : Réseau privé domicile derrière la BOX, ateliers GEII...

### •MAN:

Les MAN (Metropolitan area Network) permettent de connecter plusieurs LAN proches entre eux. Ils sont étendus à l'échelle d'un campus, d'une ville, d'une entreprise.

Ex : Réseau d'une université, d'une grande entreprise

### •WAN:

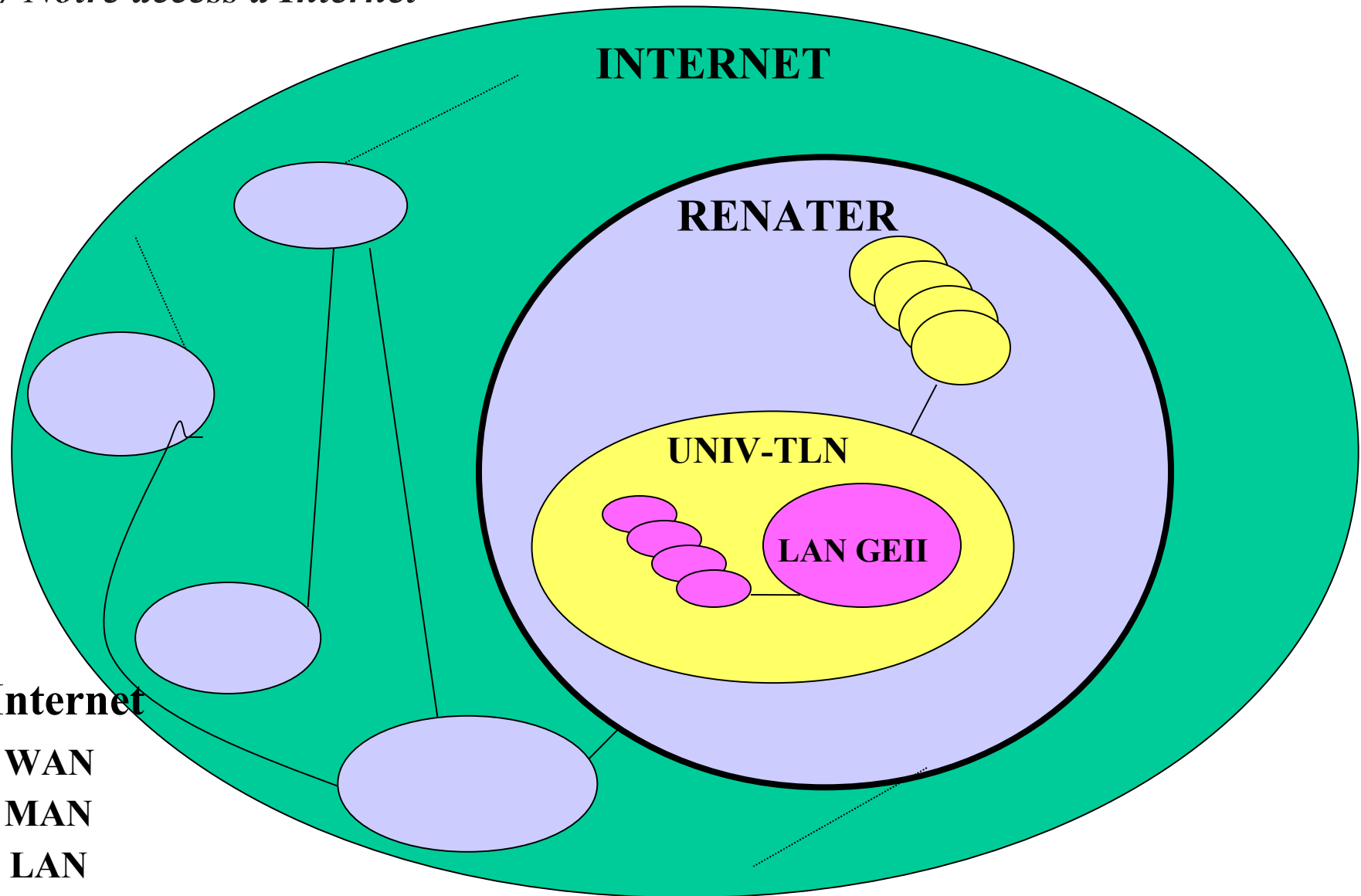
Les WAN (Wide area Network) sont des réseaux étendus à l'échelle d'une région, d'un pays.

Ex : Réseau d'un opérateur téléphonique, RENATER...

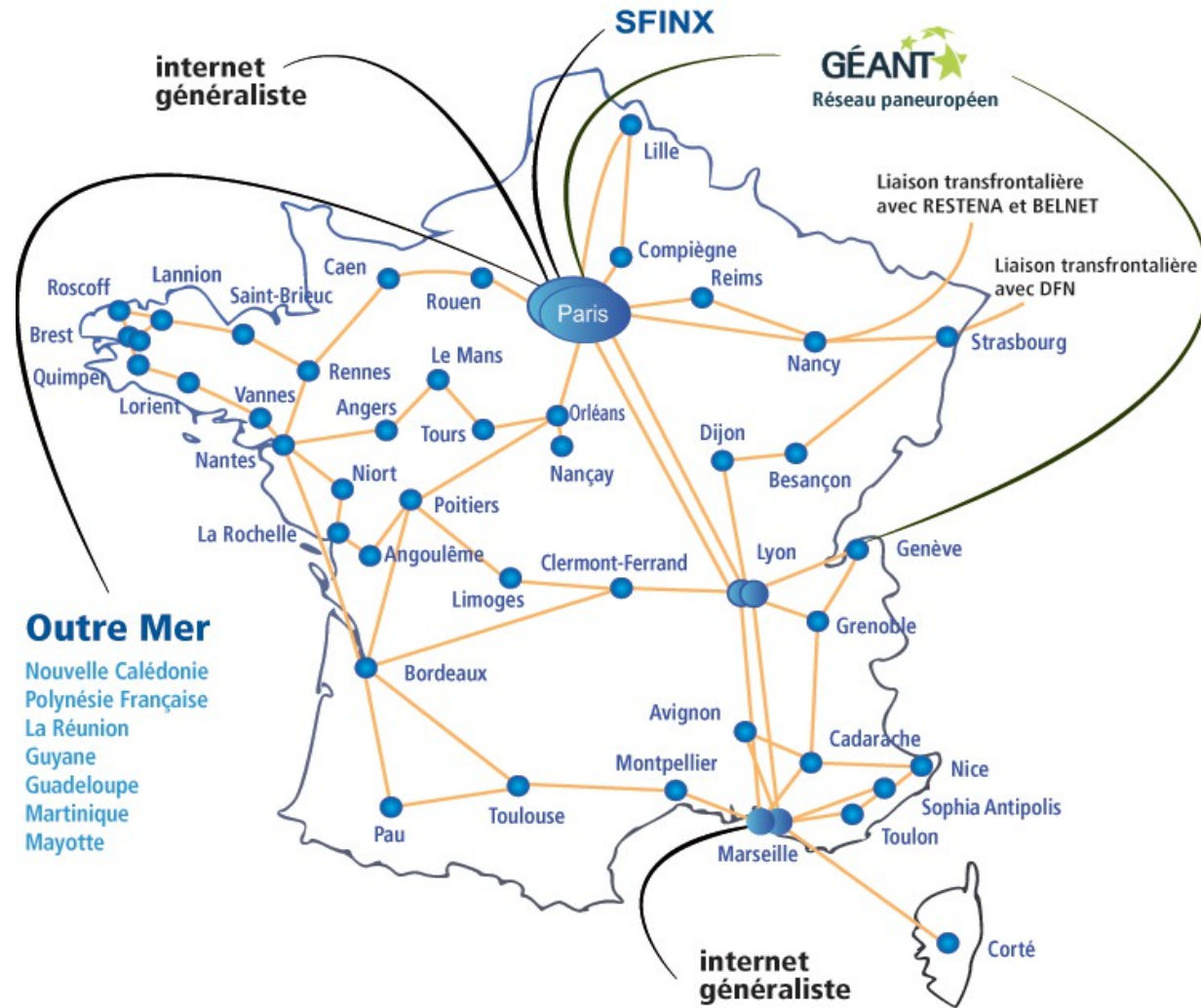
### •INTERNET:

Réseau de type WAN qui couvre la terre entière.

### *I.3.1/ Notre access à Internet*



### I.3.2/ Le réseau RENATER



## I.4/ Les topologies des réseaux locaux (LAN):

La topologie détermine la façon dont les équipements informatisés sont reliés entre eux.

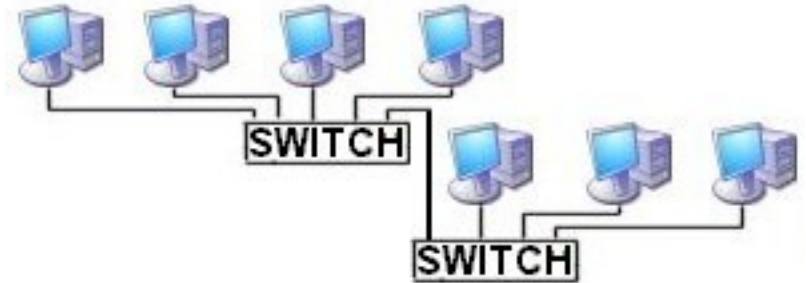
### En BUS:

Obsolète, le câble utilisé est de type coaxial.  
Ancien type de câblage pour Ethernet.



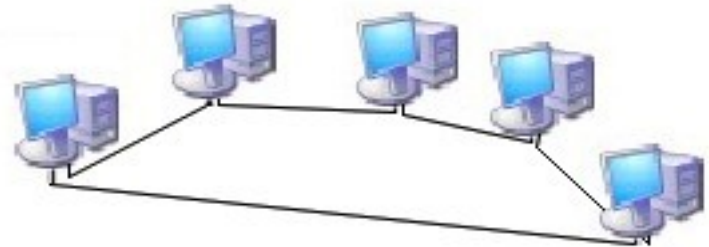
### En ETOILE:

C'est la topologie la plus utilisée. Chaque système est relié à un switch par l'intermédiaire d'un câble avec un connecteur RJ-45. Ethernet



### En ANNEAU:

Obsolète, type TOKEN RING.





## **I.5/ Les normes ou protocoles**

Pour que des personnes différentes puissent communiquer, elles doivent avoir le même langage. Pour des systèmes informatisés, c'est la même chose, on parlera alors de **protocole**.

**Un protocole est une description formelle de règles et de conventions à suivre dans un échange d'informations, que ce soit pour acheminer les données jusqu'au destinataire ou pour que le destinataire comprenne comment il doit utiliser les données qu'il a reçu.**

### *1.5.1/ Exemple d'une trame météo sur une liaison série:*



!!253\*196\*+211\*1014\r\n

Si on ne connaît pas le protocole de communication il sera impossible de recevoir et d'interpréter cette trame!

#### Protocole pour recevoir la trame :

Norme RS232,  
9600Bps  
8Bits  
no parity  
1 stop

## Protocole pour interpréter la trame:

Transmission en ASCII

!! début de trame

\r\n fin de trame

\* caractère séparateur de champ

1er champ : vitesse instantanée du vent \*10km/h

2em champ : vitesse moyenne du vent \*10km/h

3em champ : température \*10 Degré Celcius avec signe + ou -

4em champ : pression atmosphérique mb

Maintenant il est possible d'interpréter cette trame :

La vitesse instantanée du vent est de 25.3Km/h, la vitesse moyenne du vent est de 19.6Km/h, la température est de 21.1°C et la pression atmosphérique est de 1014mb.

**NB :** Cette trame a une taille variable, imaginez un protocole avec une taille fixe et sans caractère séparateur?

Pour avoir une trame de taille fixe, on peut déterminer la taille de chaque champ à 4 octets, le protocole pour interpréter la trame devient :

Transmission en ASCII

!! début de trame

\r\n fin de trame

1er champ : 4 octets

2em champ : 4 octets

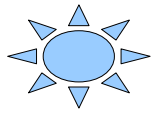
3em champ : 4 octets

4em champ : 4 octets

La trame correspondante est:

!!02530196+2111014\r\n

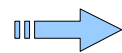
## I.6/ Transmettre de l'information



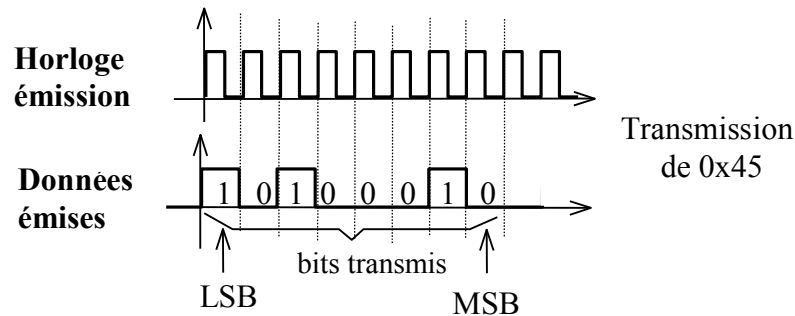
**Deux solutions:**

- En série
- En parallèle

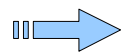
**En série:** Les bits sont émis les uns à la suite des autres sur le support de transmission au rythme d'une horloge



De plus en plus utilisée



**En parallèle:** Le support de transmission est un bus, tous les bits du mot sont transmis en même temps.



Tend à devenir obsolète

## *1.6.1/ Transmettre de l'information en série*

- Les deux systèmes n'ont pas la même horloge: **Série Asynchrone**
  - Un seul caractère (7 ou 8 bits) est transmis à la fois
  - Le rendement et le débit sont faibles
- Le récepteur et l'émetteur sont synchronisés sur la même horloge: **Série synchrone**
  - La trame peut comporter plusieurs centaines d'octets
  - L'horloge est rarement transmise sur un fil séparé, elle est synchronisée par le récepteur.
  - Un codage de donnée particulier évite qu'elle ne se désynchronise pendant la transmission.

Synchronisation de  
l'horloge du récepteur  
avec celle de l'émetteur

adresse de l'émetteur  
et du récepteur , etc.

détection des erreurs,  
caractères de fin de trame, etc.

champ de synchronisation	champ de service	<b>champ de données</b>	champ de contrôle
--------------------------	------------------	-------------------------	-------------------

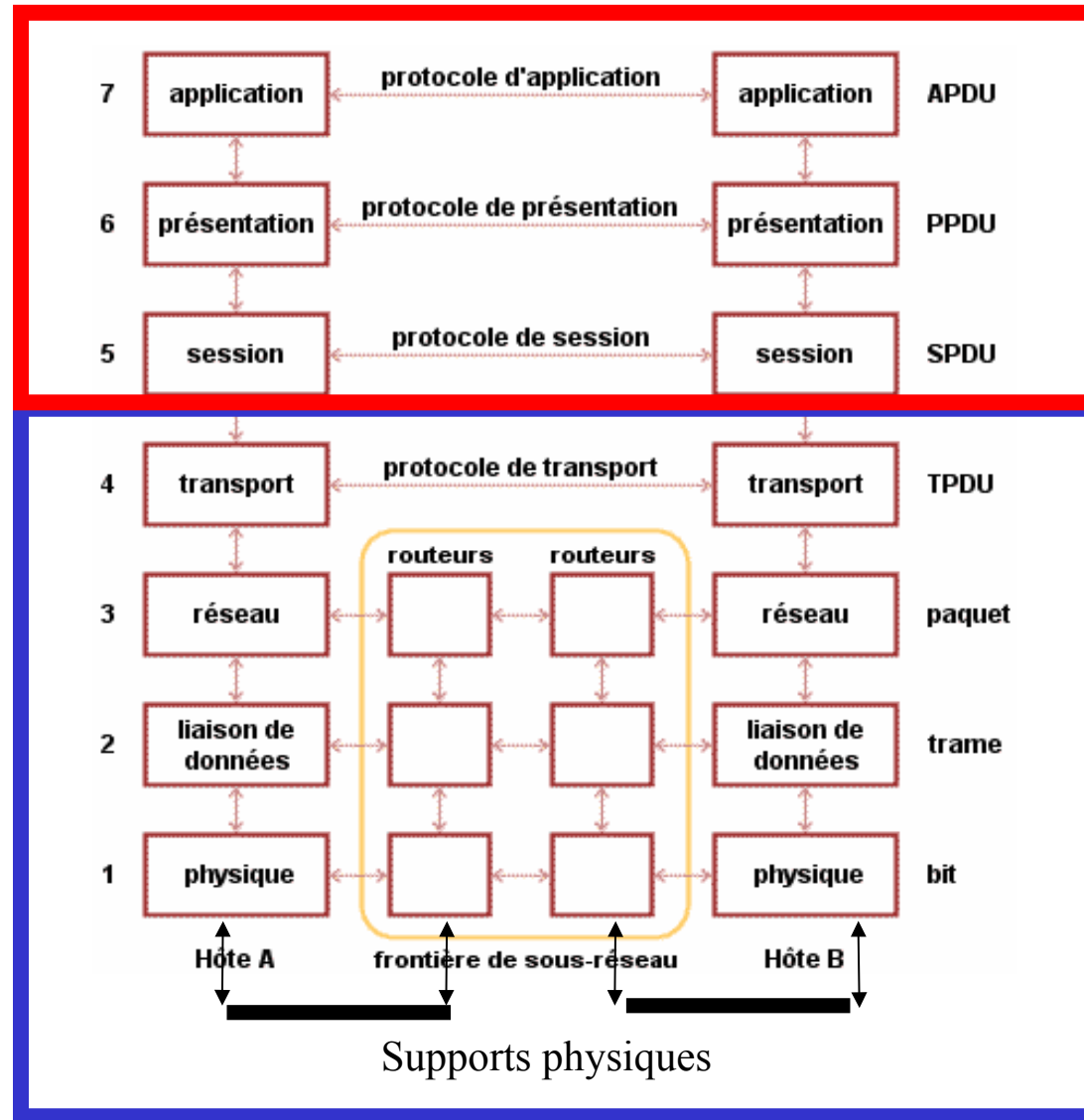
# II/ Le modèle OSI (Open Systems Interconnection)

## II.1/ Présentation

- Il décrit l'architecture en 7 couches logicielles présentant chacune des interfaces standard pour communiquer entre elles.
- Chaque couche a un rôle bien défini dans la communication
- **Virtuellement:** communication horizontale entre les couches.
- **Physiquement:** chaque couche fournit des services clairement définis à la couche immédiatement supérieure, en s'appuyant sur ceux, plus rudimentaires, de la couche inférieure, lorsque celle-ci existe.

**Les couches hautes:**  
Responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques.

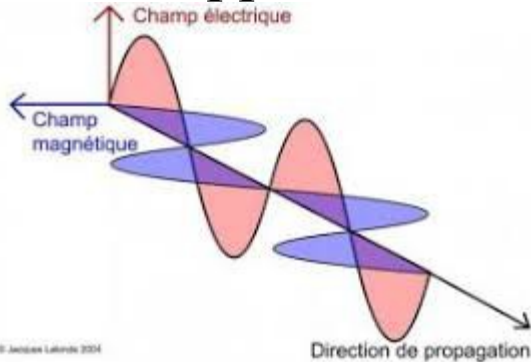
**Couches basses:**  
Acheminement des informations entre les extrémités concernées et dépendent du support physique.





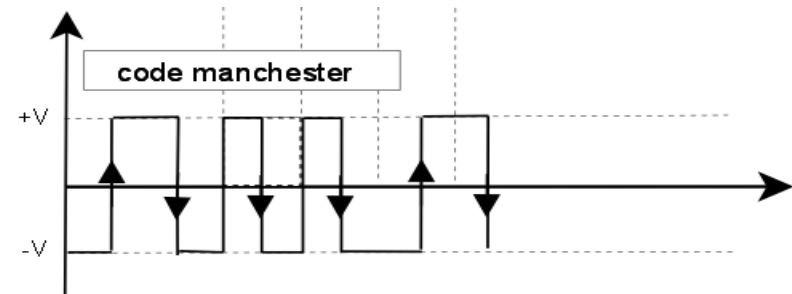
## II.2/ Description des couches 1&2

- **La couche physique** s'occupe de la transmission des bits de façon brute sur un canal de communication. C-a-d du codage/décodage d'un bit sur le support de communication

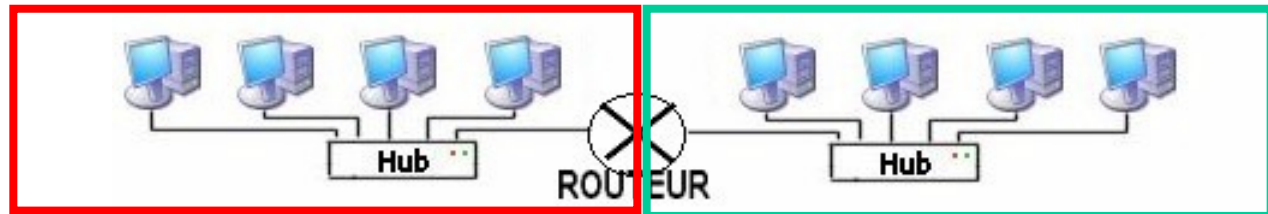


Support physique  
AIR vs CUIVRE

011101 ← **TRAME**



- **La couche liaison de données** a pour rôle de transmettre les données (**la trame**) de façon fiable entre des équipements directement connectés c-a-d sur le même sous réseau.



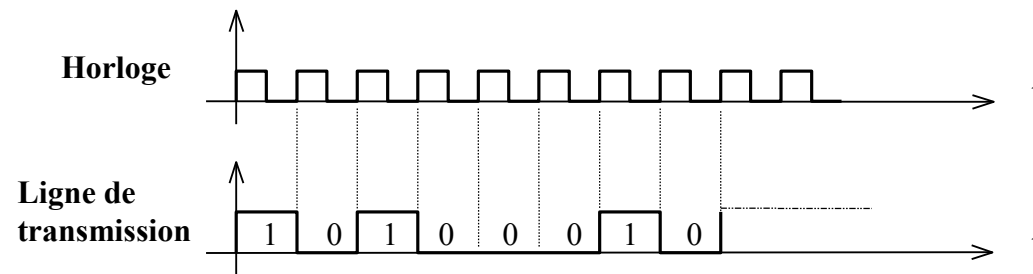
**Le rôle des couches 1&2 est assuré par l'interface Ethernet ou WIFI**

## II.2.1/ La transmission en bande de base

Nous nous intéressons à la transmission d'éléments binaires (Transmission numérique) sur un réseau local.

Le type de transmission utilisé est dit en « **bande de base** »: l'information est directement codée par des tensions et le signal généré est transmis sur la ligne.

### Transmission directe du signal:

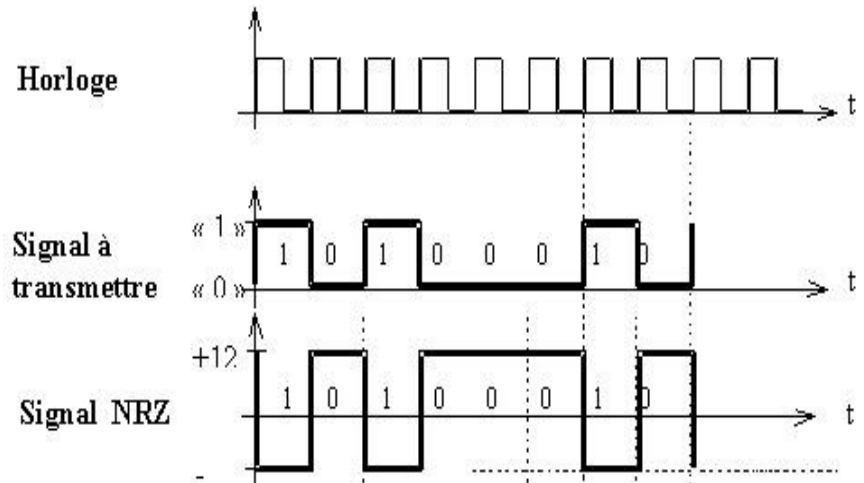


### Problèmes:

- confusion de l'état 0 volt avec rupture de transmission;
- atténuation des amplitudes;
- filtrage des basses fréquences (correspondant à de longues suites de 0 ou de 1) et des hautes fréquences (débits élevés);
- synchronisation des horloges;

## Codage en NRZ:

Utilisé dans la liaison série asynchrone type V24, RS232



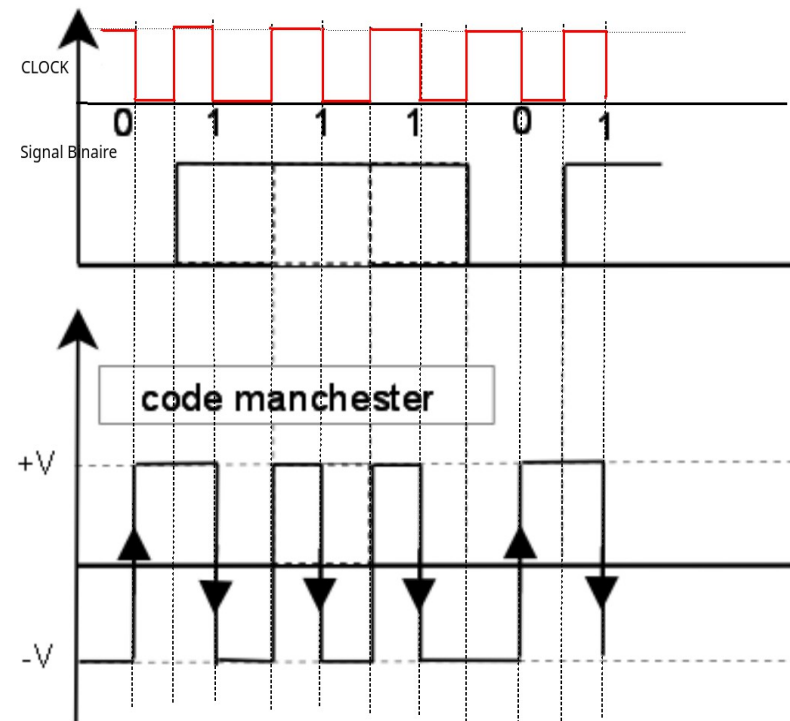
## Codage Manchester:

Not XOR entre l'horloge et le signal à transmettre (Ethernet).

Il y a toujours un front à la  $\frac{1}{2}$  période d'horloge.

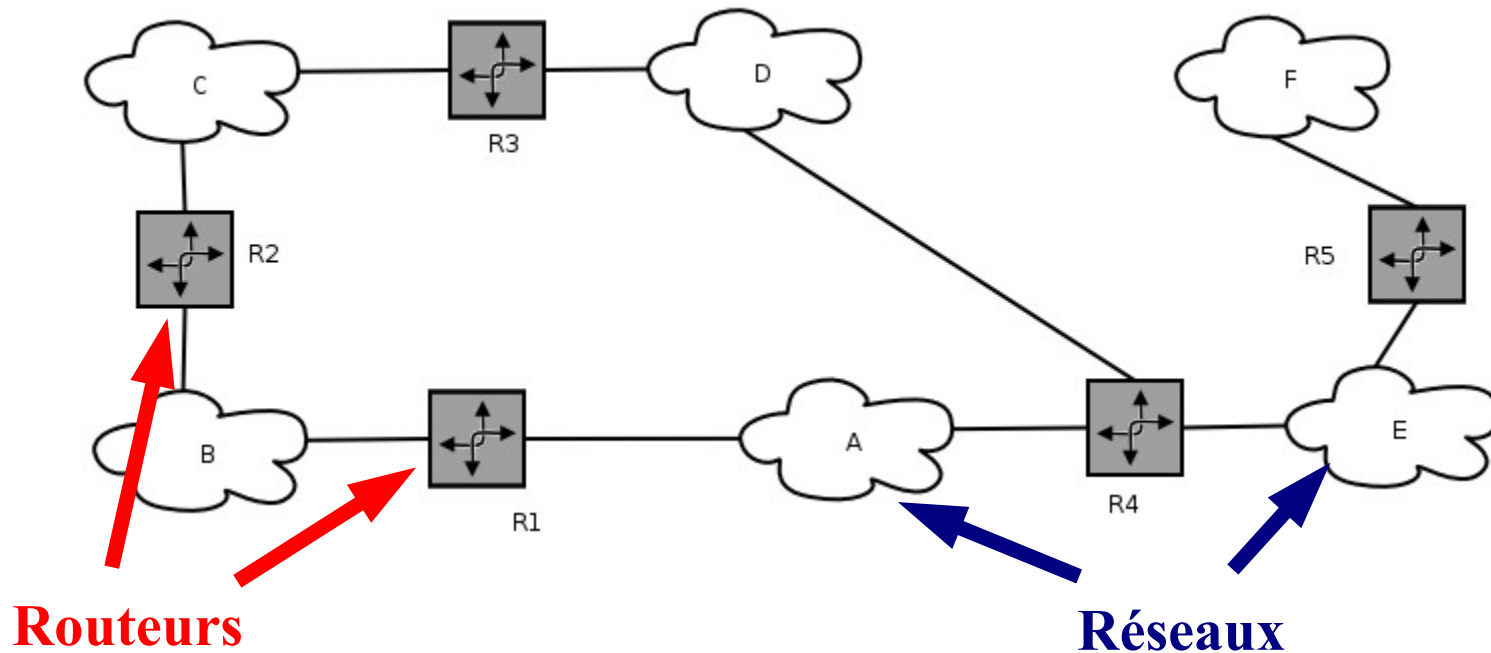
Montant  $\rightarrow$  0

Descendant  $\rightarrow$  1



## II.3/ Description de la couche 3

- La couche réseau détermine le chemin que doivent emprunter les **paquets** (routage des paquets).
  - Les différents réseaux sont reliés entre eux par des routeurs.
- Une table de routage détermine quel est le réseau destinataire du paquet.



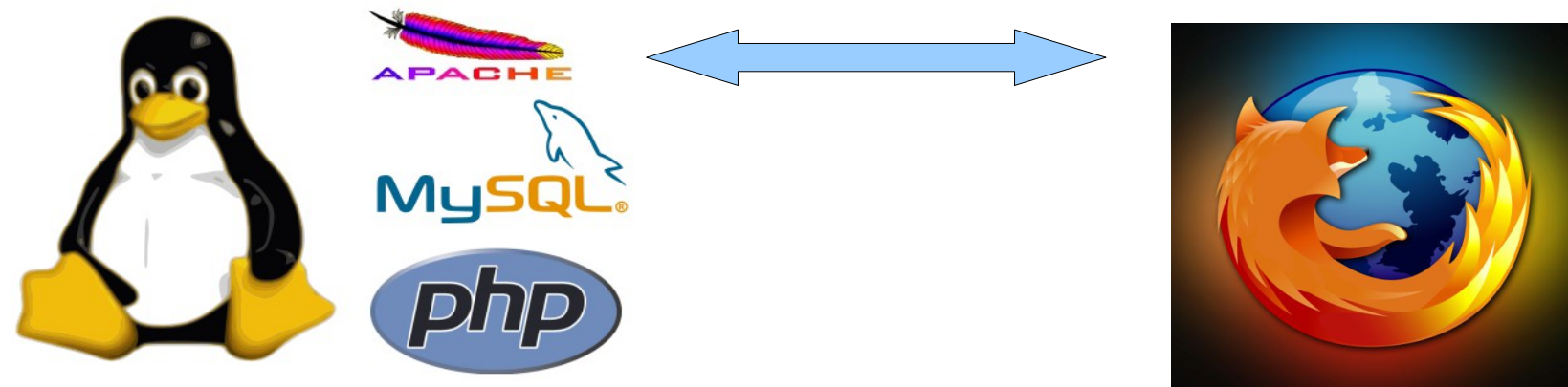
**Le plus souvent la couche 3 est Internet Protocol (IP)**

## II.4/ Description de la couche 4

- La couche Transport assure la connexion sans erreur de bout en bout entre les deux applications (processus) communicantes.
- Les informations qui transitent sont appelées **datagrammes**.

**Serveur WEB**

**Client WEB**



Les processus communicants sont repérés par un numéro (port)

Le plus souvent la couche 4 est Transport Control Protocol (TCP)

## II.5/ Les couches hautes

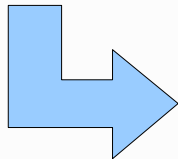
Les couches 5,6&7 sont dites applicatives:

HTTP Hyper Text Transfert Protocol

FTP File Transfert Protocol

...

En informatique industrielle nous devons souvent créer une application dédiée, couches 5,6&7, bâtie sur les couches basses (généralement la pile TCP/IP).



## Programmation réseau

# III/ Ethernet

## III.1/ Présentation

Ethernet est une technologie pour les réseaux locaux développée au début des années 70 à Xerox PARC (Palo Alto Research Center). Elle est standardisée en 1978 par un consortium DIX regroupant Digital, Intel et Xerox, puis normalisée par l'IEEE, sous les numéros 802.3 et 802.2.

- ➡ Débit 10 Mbps
- ➡ Codage Manchester
- ➡ Tension (+0,85V/-0,85V)

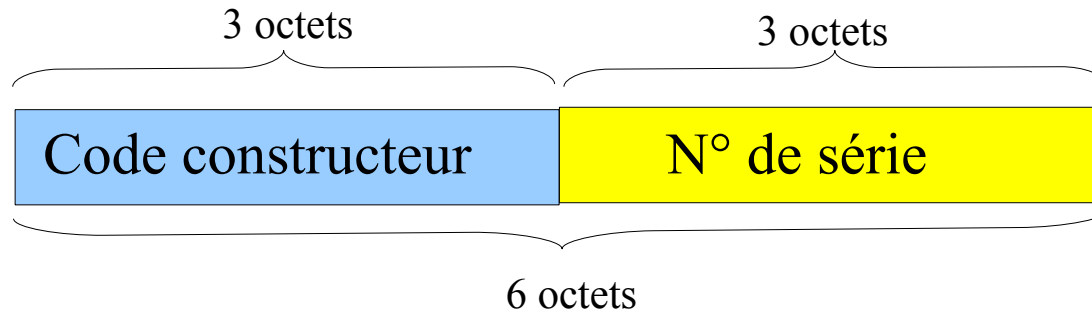
1995 passage au débit 100Mbps et Auto-négociation 10/100Mbps

1998 passage au débit 1Gbps

2002 débit de 10Gbps

## III.2/ L'adressage sur Ethernet

Sur Ethernet chaque station est repérée par une adresse unique au monde. Cette adresse (on parlera de MAC address) est représentée sur 6 octets.



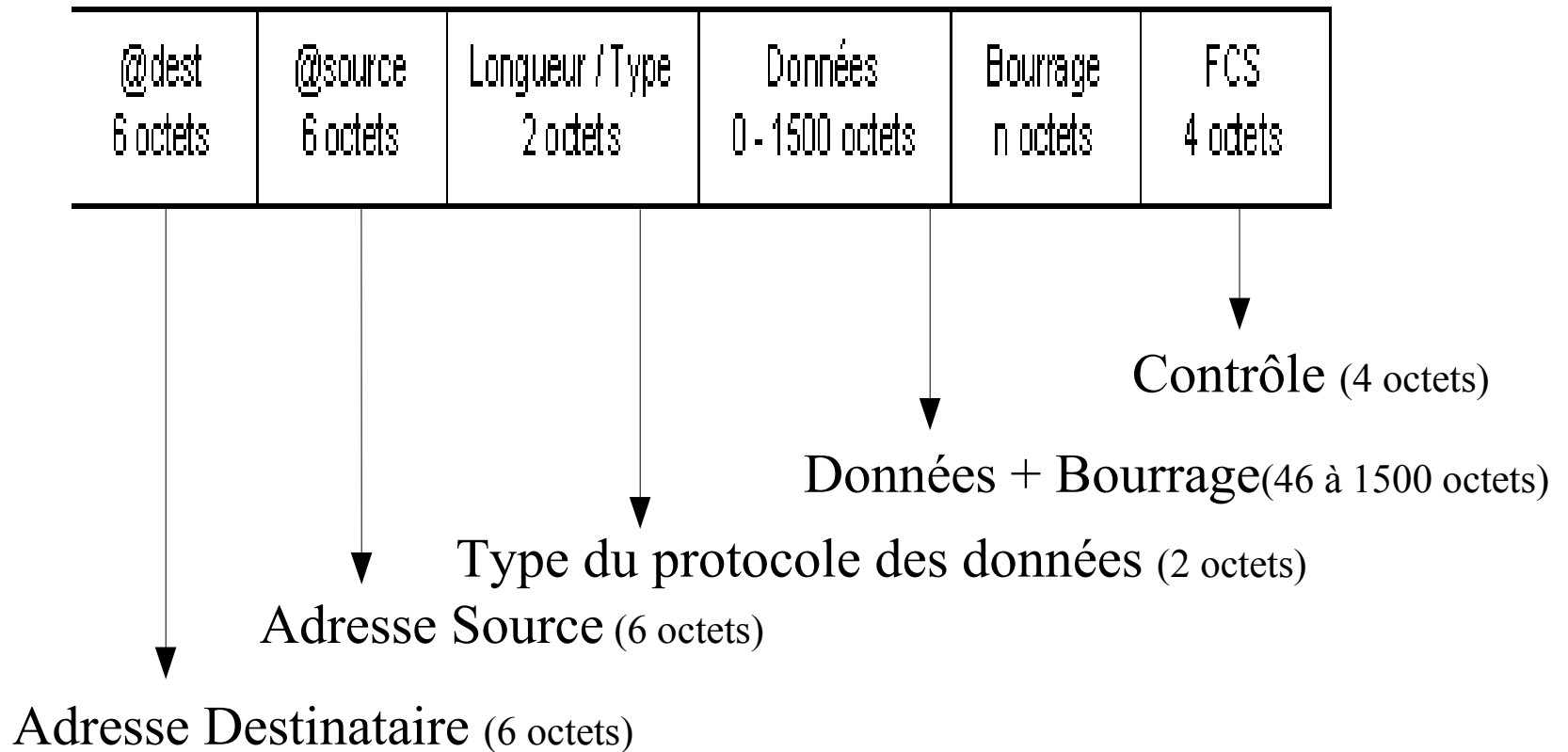
**Ex:** 00-00-0C-F2-00-12 est l'adresse d'une carte CISCO

 FF-FF-FF-FF-FF-FF est une adresse de diffusion, c-a-d toutes les machines sur le sous réseau sont considérées comme destinataires

Pour trouver tous les codes constructeurs: <http://standards.ieee.org/regauth/oui/index.shtml>



### III.3/ La trame Ethernet



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14 ... 1513	1514	1515	1516	1517
Adresse MAC destination						Adresse MAC source						Type de protocole		Données	FCS/CRC			

♦ Avec pour le champs Type de protocole de données les valeurs :

- \* 0x0800 :IPv4
- \* 0x86DD :IPv6
- \* 0x0806 :ARP
- \* 0x8035:RARP
- \* 0x0600:XNS
- \* 0x809B:AppleTalk

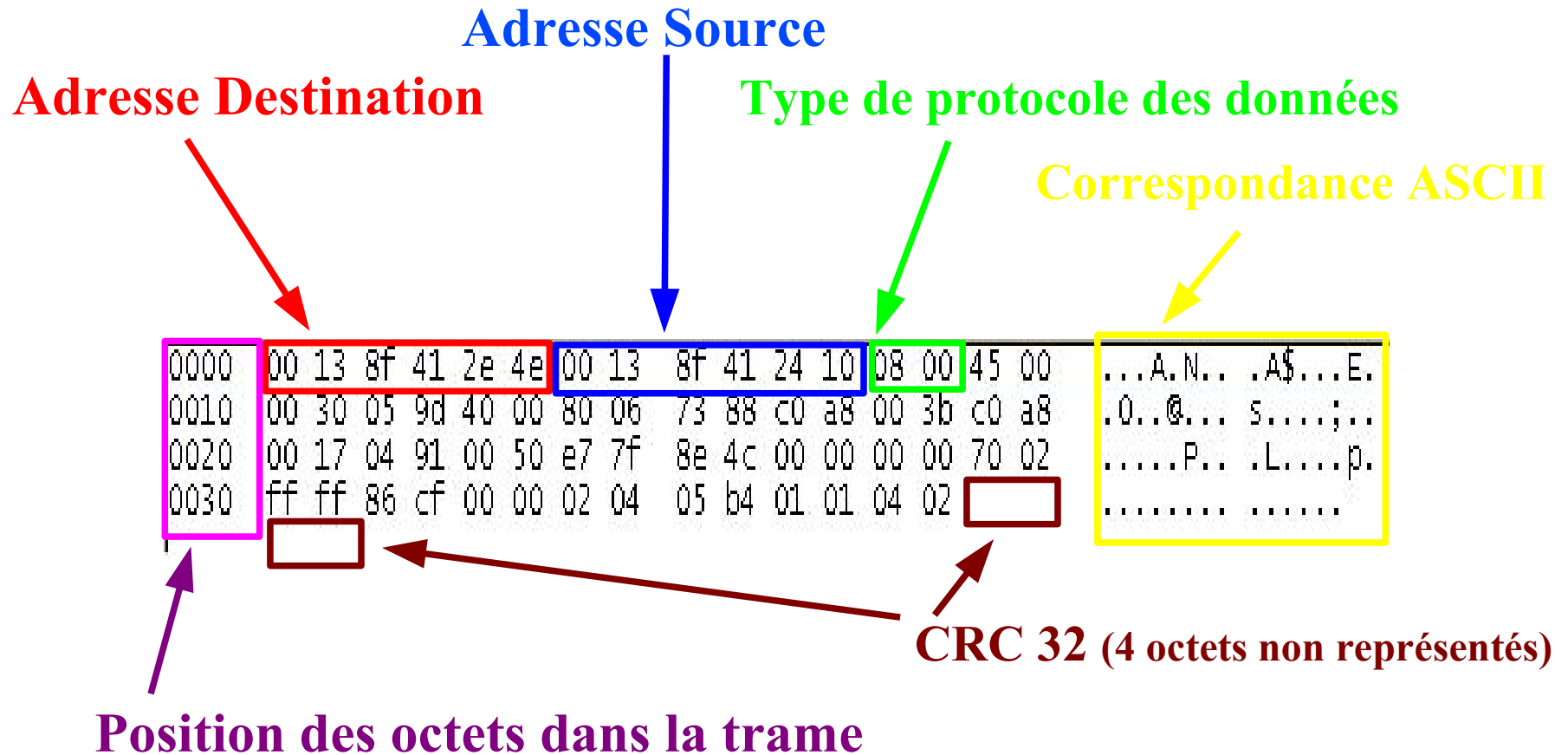
## Taille de la trame (avec CRC):

**Min:** 64 octets

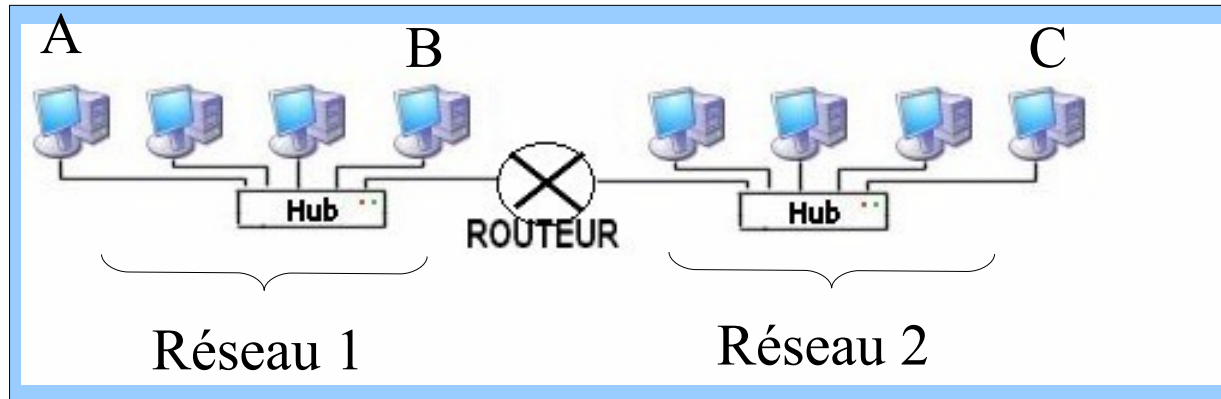
**Max:** 1518 octets

Si la trame est trop petite des octets sont ajoutés dans la zone des données (bourrage) pour arriver à la taille minimale de 64 octets.

### III.3.1/ Capture WIRESHARK de la trame Ethernet



### III.4/ Domaine de visibilité de l'adresse MAC



#### Communication de A vers B: routage direct

1 Trame sur le réseau1: @Source: @MAC de A  
@Dest: @MAC de B

#### Communication de A vers C: routage indirect

1 Trame sur le réseau1: @Source: @MAC de A  
@Dest: @MAC du Routeur sur réseau1  
1 Trame sur le réseau2: @Source: @MAC du Routeur sur réseau2  
@Dest: @MAC de C

**Routage direct :** les deux machines sont sur le même réseau

**Routage indirect :** les deux machines ne sont pas sur le même réseau, le paquet passera par au moins un routeur.

### III.5/ Méthode CSMA/CD: Algorithme simplifié

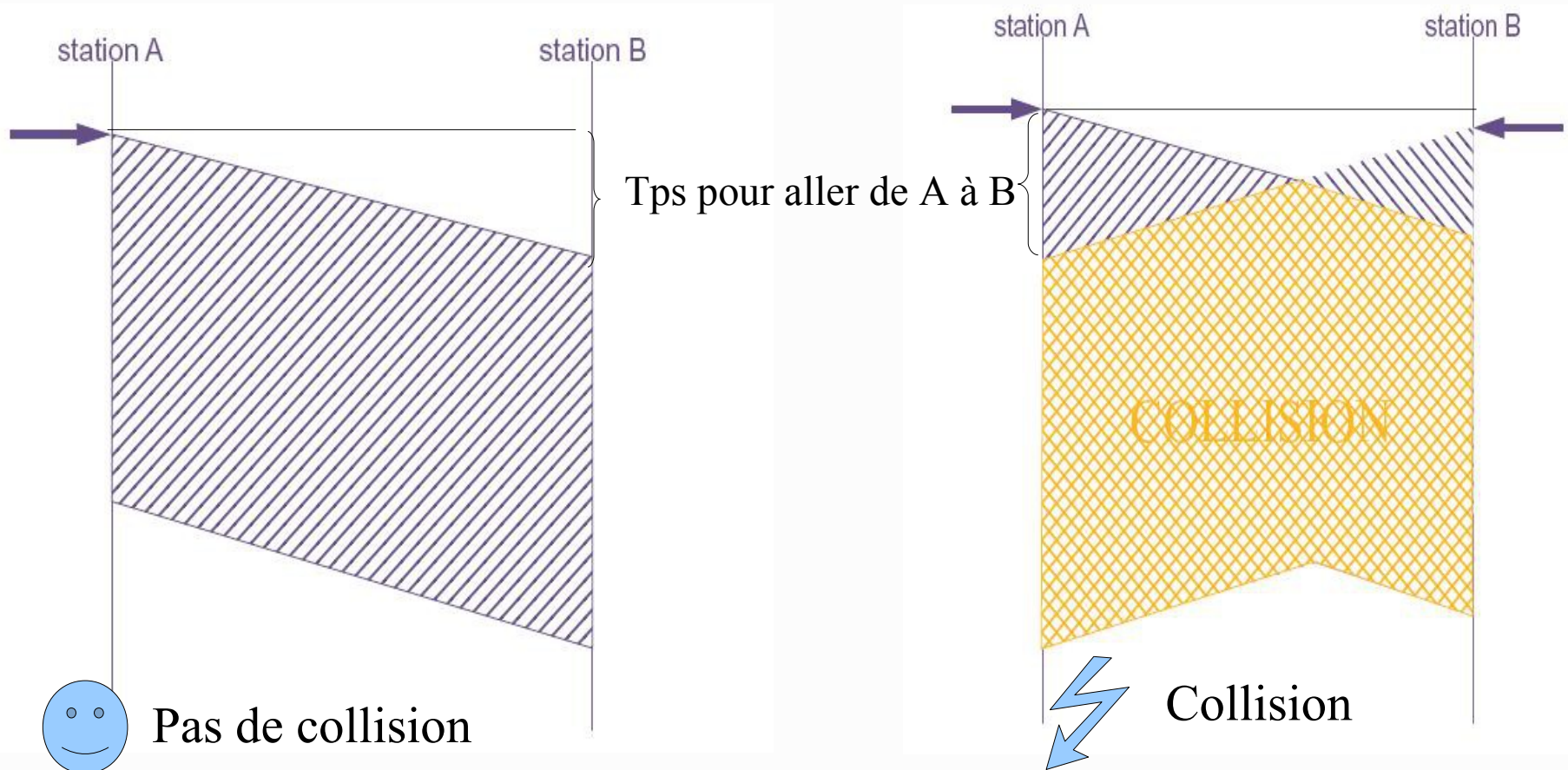
CSMA/CD est la méthode d'accès au support:

- 1/ Si le canal est libre, alors émettre une trame.
- 2/ Si le canal est occupé attendre sa libération et émettre dès qu'il se libère.
- 3/ Si on détecte une collision durant l'émission:
  - Arrêter l'émission
  - Attendre un temps aléatoire avant de réémettre.

### III.5.1/ Comment peut il y avoir collision (avant éthernet commuté)?

Sur un câble Ethernet la vitesse du signal est de  $0,77C = 230\,000\text{ Km/s}$

Avec  $C$  = vitesse de la lumière dans le vide

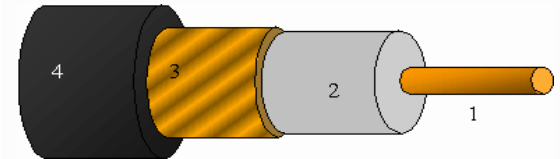


## III.6/ Le câblage Ethernet

Pour une spécification telle que **XBaseY** :

- \* X représente le débit du réseau en megabits/seconde (Mbps)
- \* Y représente le type de connexion utilisée
- \* Base signifie: codage en bande de base

**10Base2:** 10Mbit/s sur câble coaxial de 50 ohms segment max de 185m (obsolète). Un maximum de 5 segments reliés par des répéteurs.

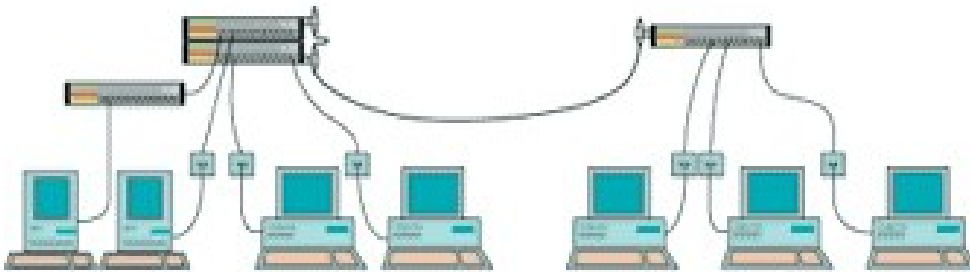


Tendance actuelle: Un concentrateur (ou hub) ou un commutateur (ou switch) est au centre du réseau, avec un port pour chaque nœud.

## 10 BaseT: Ethernet sur paire torsadée (Twisted)

- Câble à paires torsadées, de préférence catégorie 5 (connectique RJ45)
- 100m Max entre 2 HUB ou station vers HUB
- Un max de 4 HUB entre les stations

RESEAU 10baseT

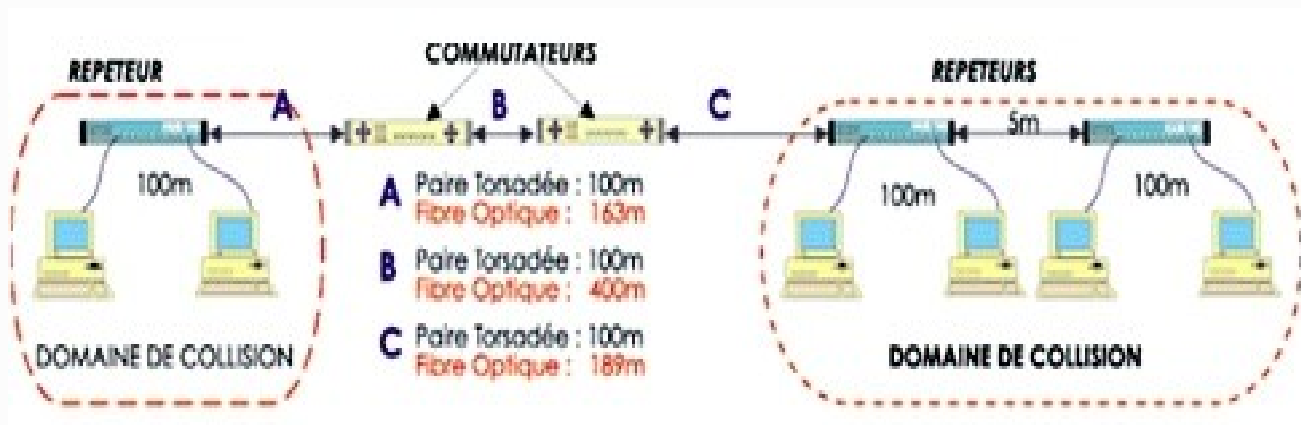


	Male	Female
RJ45	8 1 	1 

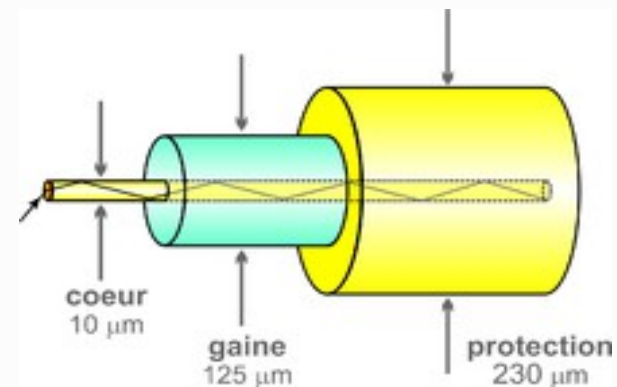




## Fast Ethernet: 100BaseT ou 100Base Fx (Fibre optique)



Le standard actuel est le GIGABIT Ethernet (1000 Mbps) sur paire torsadée ou fibre optique.



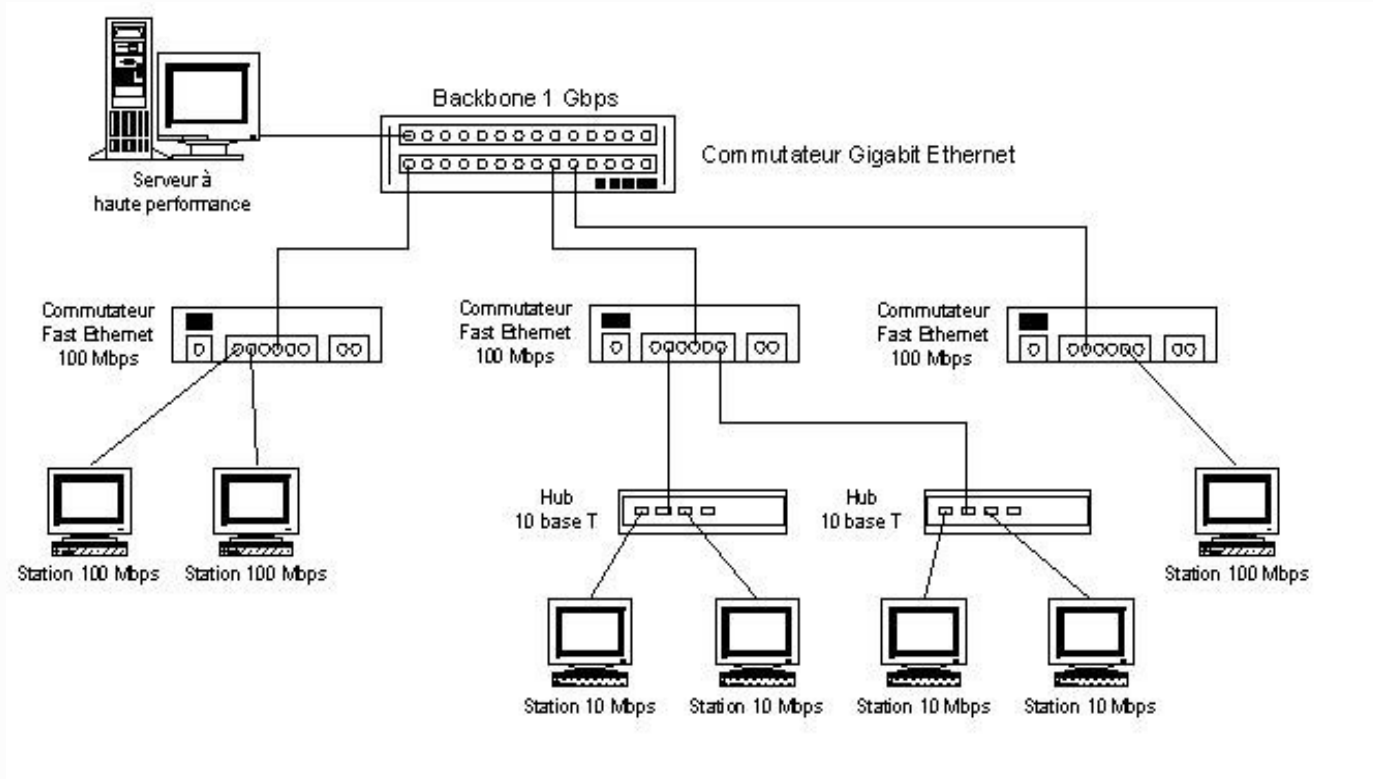
Sigle	Dénomination	Câble	Connecteur	Débit	Portée
10Base2	Ethernet mince (thin Ethernet)	<a href="#">Câble coaxial</a> (50 Ohms) de faible diamètre	BNC	10 Mb/s	185m
10Base5	Ethernet épais (thick Ethernet)	Câble coaxial de gros diamètre (0.4 inch)	BNC	10Mb/s	500m
10Base-T	Ethernet standard	Paire torsadée (catégorie 3)	RJ-45	10 Mb/s	100m
100Base-TX	Ethernet rapide (Fast Ethernet)	Double paire torsadée (catégorie 5)	RJ-45	100 Mb/s	100m
100Base-FX	Ethernet rapide (Fast Ethernet)	Fibre optique multimode du type (62.5/125)		100 Mb/s	2 km
1000Base-T	Ethernet Gigabit	Double paire torsadée (catégorie 5e)	RJ-45	1000 Mb/s	100m
1000Base-LX	Ethernet Gigabit	Fibre optique monomode / multimode		1000 Mb/s	550m /10000m
1000Base-SX	Ethernet Gigabit	Fibre optique multimode		1000 Mbit/s	550m
10GBase-SR	Ethernet 10Gigabit	Fibre optique multimode		10 Gbit/s	500m
10GBase-LX4	Ethernet 10Gigabit	Fibre optique multimode		10 Gbit/s	500m

Half duplex : 1 paire  
Full duplex : 2 paires  
Débit >= 1Gbps : 4 paires

10GBase-T | Ethernet 10 Giga | 4 Paires torsadées (cat 6) | RJ45 | 10 Gbit/s | 100m

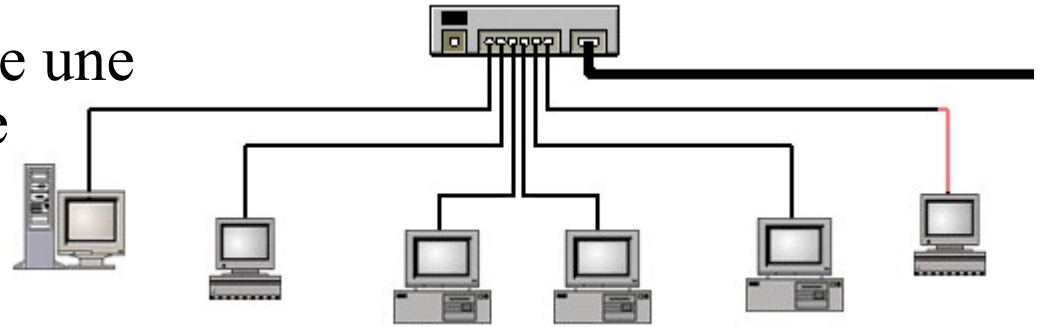
Le nouveau standard Ethernet 10 Gigabits entoure plusieurs types de médias différents pour les réseaux locaux, réseaux métropolitains et réseaux étendus.

### III.6.1/ Exemple d'architecture Ethernet câblée

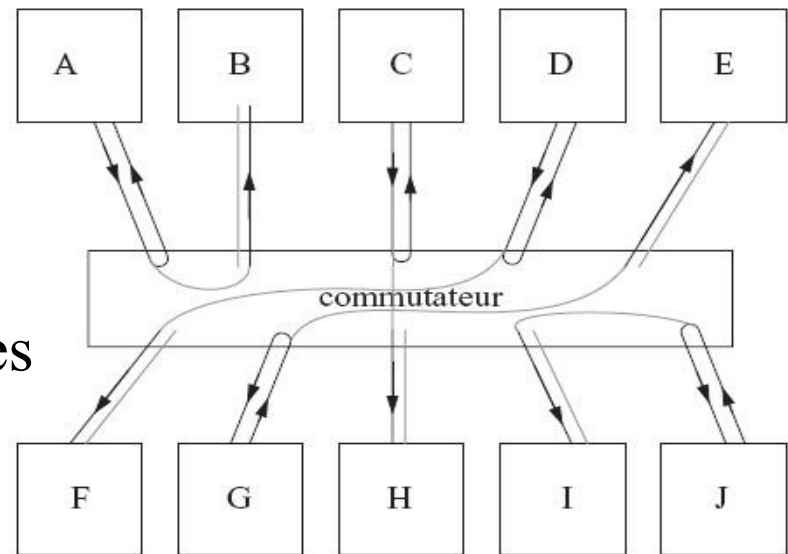


### III.7/ HUB ou SWITCH?

Un HUB (concentrateur) réalise une émulation de BUS et fait office de répéteur.



Un switch (commutateur) réalise un aiguillage sur la base des adresses MAC destinataires.



## Commutation cut-through

Elle démarre le processus propagation à partir de l'adresse MAC du destinataire avant que la totalité de la trame soit reçue. Avec ce modèle, les temps d'attente sont aussi courts quelle que soit la longueur des trames. Cependant, les trames erronées sont transmises sans aucun contrôle.

## Commutation store and forward

La totalité de la trame est lue et validée avant sa retransmission. Ceci permet de supprimer les trames corrompues et de définir des filtres pour contrôler le trafic à travers le commutateur. Les temps d'attente augmentent avec la longueur des trames.

Il est possible pour une station que son port soit saturé en réception par plusieurs communications entrantes. Le commutateur peut alors stocker temporairement et/ou détruire les trames qui ne peuvent être transmises, ou générer un signal de collision factice vers la station émettrice.

# IV/ Le WIRELESS

## IV.1/ Généralités

**Wireless** : Désigne un réseau sans fil (qui n'utilise pas de câbles). Le support est l'air, l'information transite par le biais d'ondes électromagnétiques.

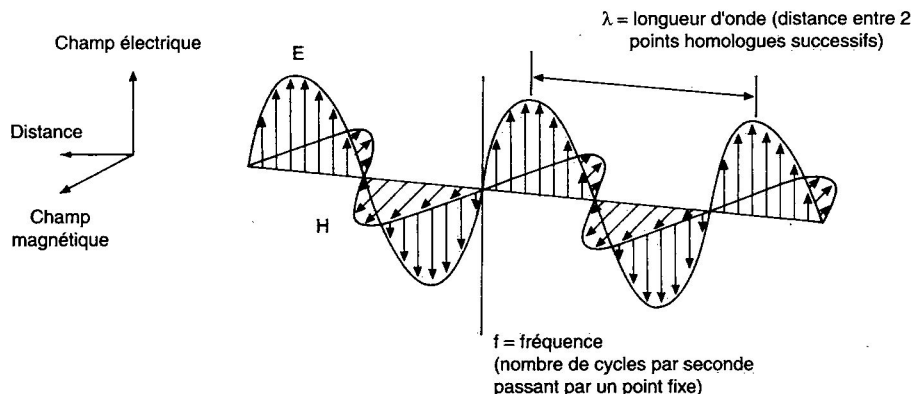
**Ondes électromagnétiques** : C'est la résultante d'un champ électrique et d'un champ magnétique dont les amplitudes varient de façon sinusoïdale au cours du temps.

- Vitesse de propagation : Dans l'air, proche de  $3 \times 10^8 \text{ ms}^{-1}$
- Fréquence et Période : pour un signal à 2.4GHz la période sera de  $4.16 \times 10^{-10} \text{ s}$
- Longueur d'onde : C'est la distance parcourue pendant une période :

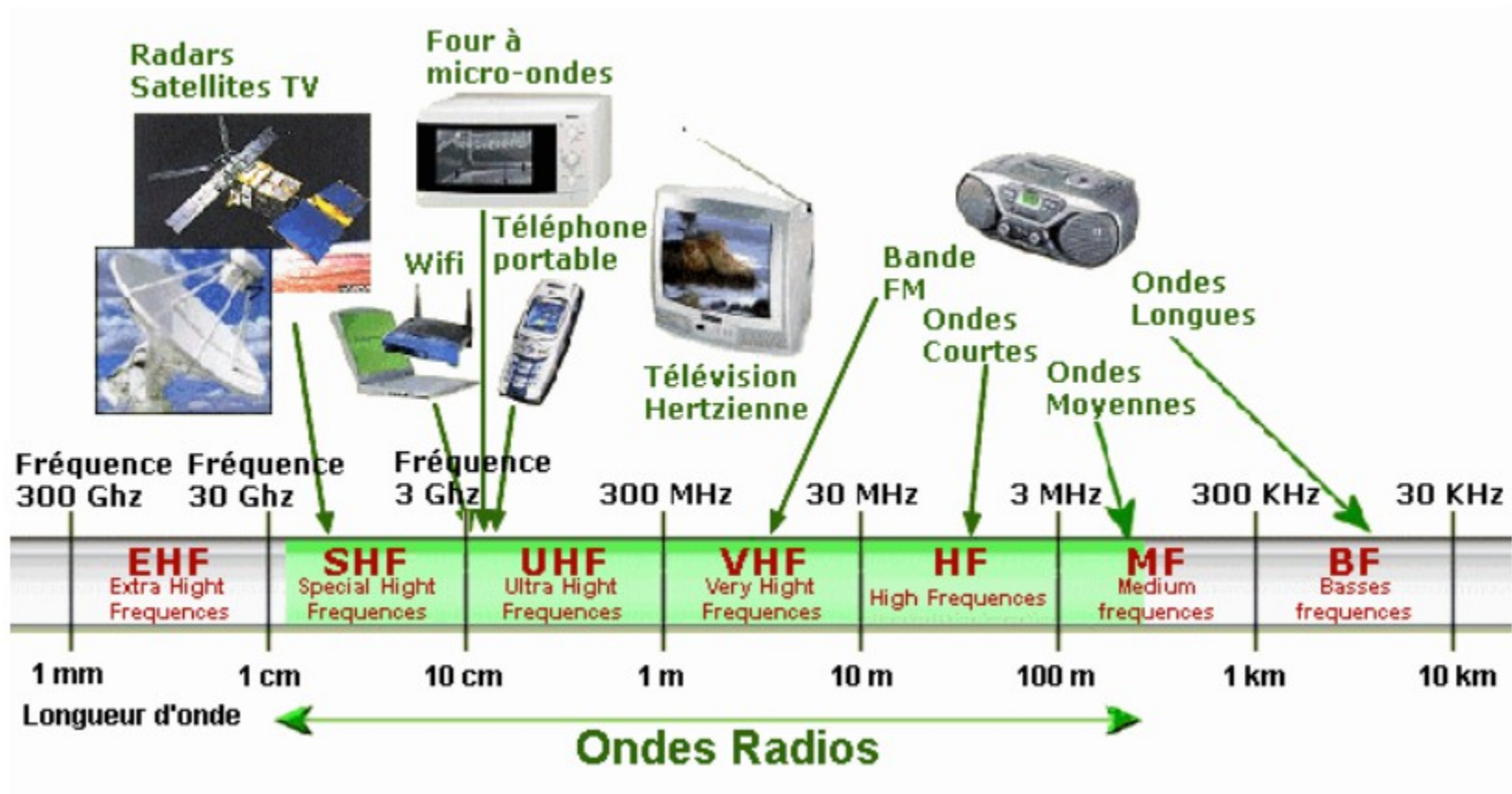
Toujours pour un signal à 2.4GHz dans l'air :

$$L = 3 \times 10^8 \text{ ms}^{-1} \times 4.16 \times 10^{-10} = 12.48 \times 10^{-2} \text{ m} = 12.48 \text{ cm}$$

➤ Un objet peut constituer un obstacle à la propagation d'une onde lorsque cet obstacle atteint une dimension supérieure ou égale à la longueur de l'onde.



## IV.2/ Utilisation des ondes électromagnétiques



**Risques sanitaires :** Il faut garder à l'esprit que les ondes électromagnétiques sont potentiellement dangereuses il est conseillé, dans la mesure du possible, de limiter l'exposition.





## IV.3/ Classification des réseaux sans fils

	WPAN	WLAN	WMAN	WWAN
Nom commun	Bluetooth et autres	WiFi	WiMax	GSM, GPRS, UMTS
Bande de fréquence	2,4 GHz	2,4 / 5 GHz	2 – 11 GHz	900 / 1800 MHz 1900 / 2200 MHz
Portée	qq m	100 m	50 km	35 km
Débit théorique	3 Mb/s	54 Mb/s	70 Mb/s	9600 Kb/s -> 2 Mb/s
Applications	Connexion périphériques	Réseau local	Accès	Téléphonie et données
Norme	IEEE 802.15	IEEE 802.11	IEEE 802.16	ITU





## IV.4/ Les normes Wi-Fi

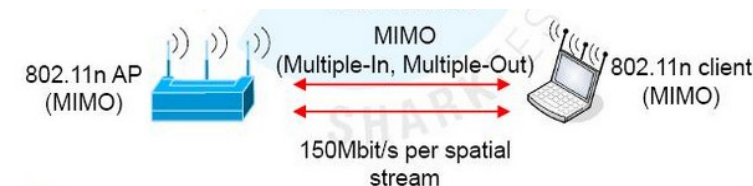


**Wi-Fi** : Contraction de Wireless Fidelity, le Wi-Fi est un ensemble de normes concernant les réseaux sans fil (famille IEEE 802.11)

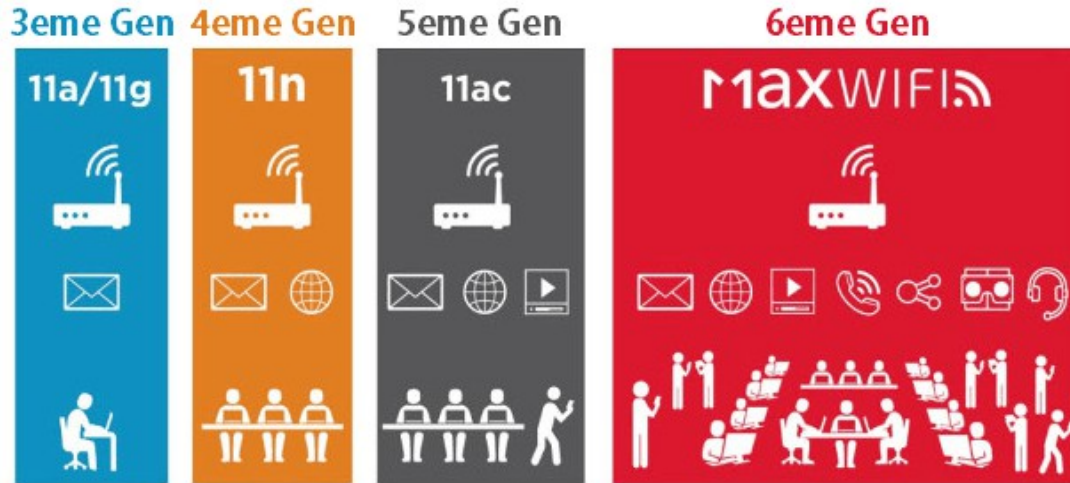
802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
a (WiFi 1)	5 GHz	54 Mbps	Faible	Faible	20 MHz	Non
b (WiFi 2)	2,4 GHz	11 Mbps	Correcte	Elevée	20 MHz	Non
g (WiFi 3)	2,4 GHz	54 Mbps	Correcte	Elevée	20 MHz	Non
n (WiFi 4)	2,4 GHz	288 Mbps	Bonne	Elevée	20 MHz	Non
n (WiFi 4)	5 GHz	600 Mbps	Correcte	Faible	20 ou 40 MHz	Oui
ac (WiFi 5)	5 GHz	5 300 Mbps	Correcte	Faible	20, 40, 80 ou 160 MHz	Oui
ad	60 GHz	6 757 Mbps	Très faible	Faible	2 160 MHz	Oui (+MU-MIMO)
ax (WiFi 6)	2,4 et 5GHz	10 530 Mbps	Correcte	Très faible	20, 40, 80 ou 160 MHz	

MU : Multi User

MIMO : Multiple Input, Multiple Output

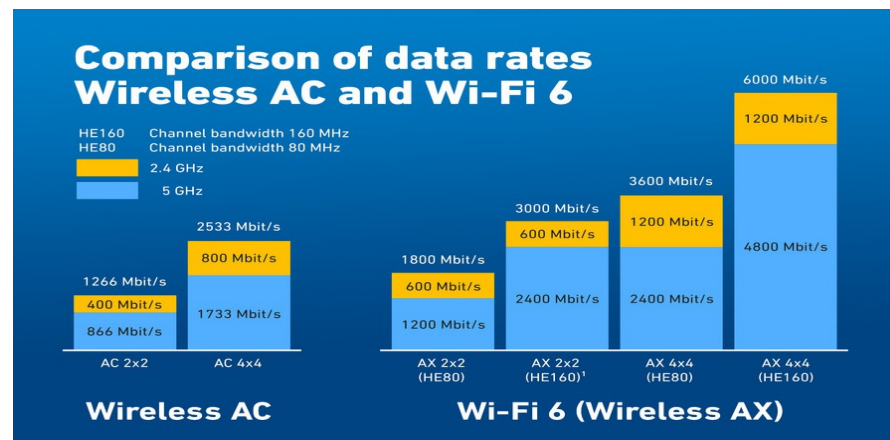


# L'Evolution du WiFi



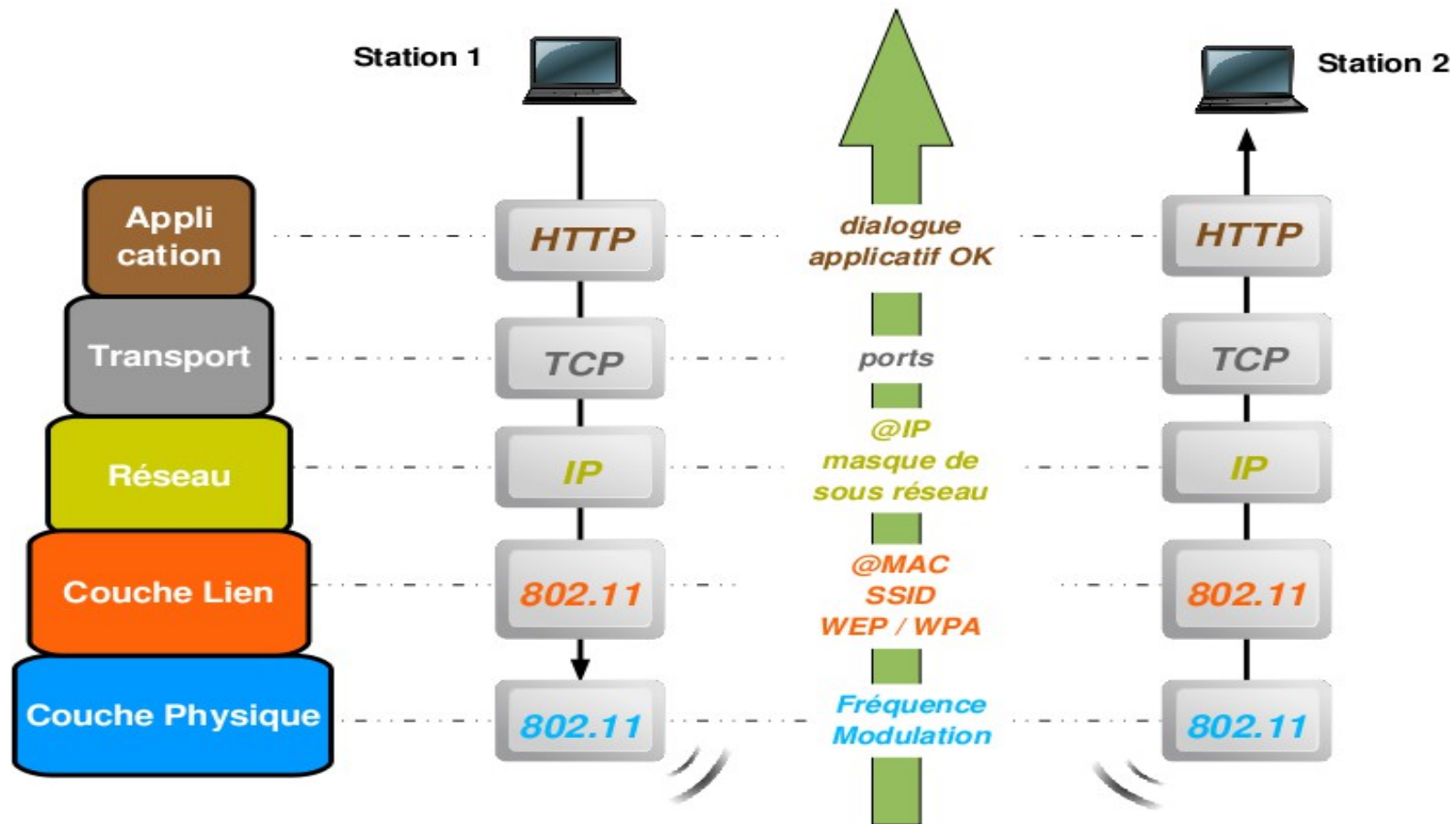
Nouvelle norme WiFi 6  
(802.11 ax)

- ✓ Débit \* 4 par rapport à la génération, précédente même en zone dense (4.6 Gbps)
- ✓ Bande 2,4 GHz et 5 GHz (compatibilité ascendante avec les anciens matériels)
- ✓ WPA3
- ✓ Économe en énergie (mode veille quand il n'y a pas de trafic)
- ✓ Portée environ 35m



## IV.5/ Wi-Fi et modèle OSI

**IEEE 802.11** : Ces normes spécifient les couches 1&2 du modèle OSI



## IV.5.1/ Spécification de la couche 1

802.11x	Couche Liaison de données	802.2 (LLC)
		802.11 (MAC)
	Couche Physique (PHY)	DSSS FHSS Infrarouges

### Couche PHY

- **Infrarouge** : Utilise une onde lumineuse pour transmettre les données dans un seul sens et en vue directe (obsolète).

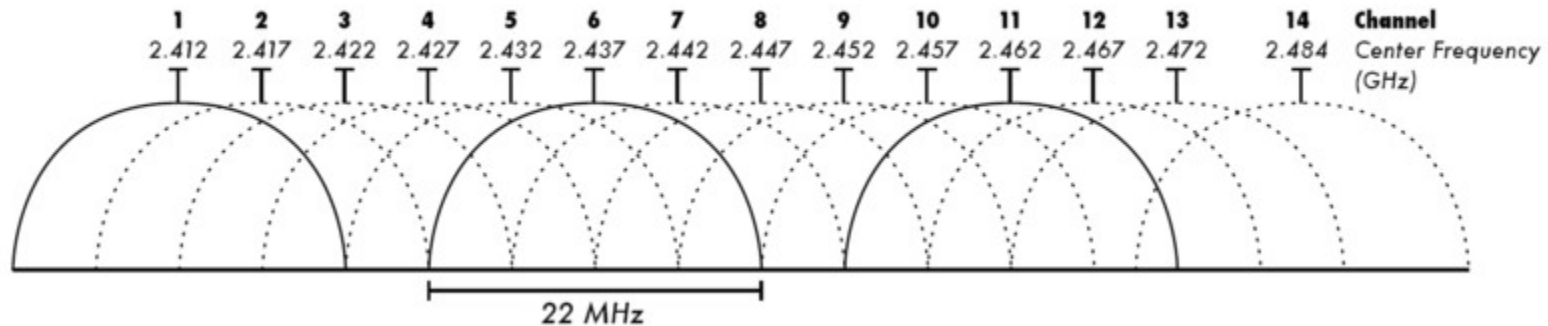
- **DSSS** : On utilise la bande ISM (Industrie, Science et Médical), elles peuvent être utilisées librement pour des applications industrielles, scientifiques et médicales.

Bande 2.4GHz : 2 400 à 2 483 MHz

Bande 5GHz : 5150 à 5725 MHz

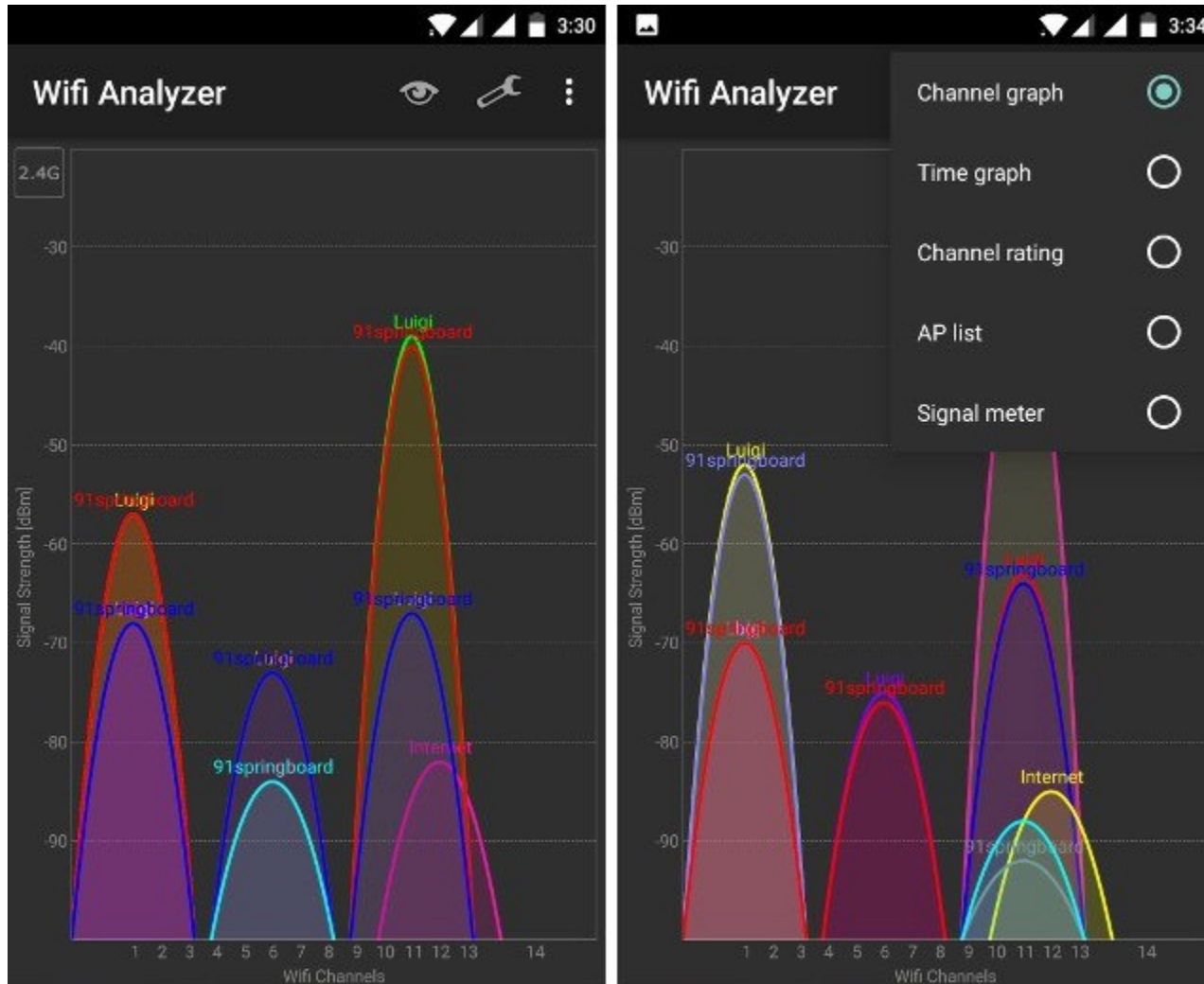
#### IV.5.2/ Bande des 2.4GHz

- 13 canaux disponibles (le 14 est interdit en France) avec recouvrements, chaque canal est centré sur une bande de fréquence de 22MHz



- Utiliser le même canal qu'un autre AP implique de partager la BP avec lui ! C'est toutefois moins pénalisant que d'utiliser un autre canal se recouvrant (détection des collisions VS parasites électro magnétiques)
- Dans ce cas on peut changer de canal en choisissant celui qui paraît le moins occupé parmi les canaux 1, 6 et 11 (attention aux chevauchements).
- **Il est déconseillé d'utiliser un autre canal que le 1, 6 ou 11**

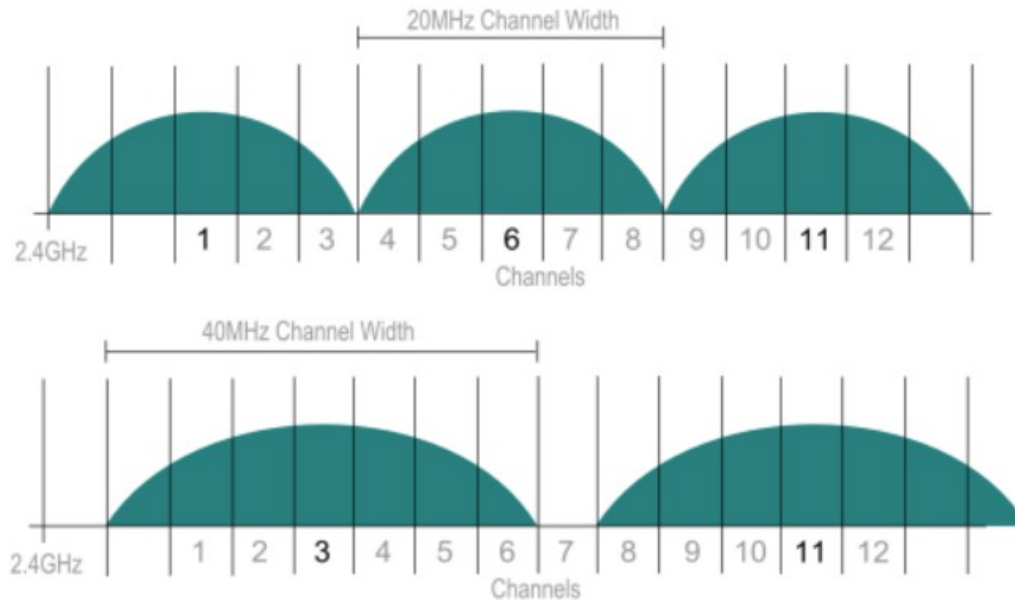
On a tout intérêt à utiliser une application gratuite sous android pour visualiser l'occupation des différentes bandes de fréquences. WiFiAnalyser est, par exemple, une application intéressante.



## 40MHz ou 20MHz ?

Sur certains AP (Acces Point 802.11n) en plus du canal on a aussi le choix entre deux bandes de fréquences :

- 20MHz (en fait 22MHz) vu précédemment
- 40MHz



Passer en 40MHz peut améliorer le débit mais aussi augmenter les interférences avec les autres canaux (A utiliser seulement dans un environnement faiblement occupé)



### IV.5.3/ Bande des 5GHz

Le wifi utilise principalement la bande de fréquence 2,4 GHz, mais celle-ci est très utilisée (par le Bluetooth également).

La norme WI-FI AC utilise la bande des 5GHz, 19 canaux et plusieurs possibilités de largeur de bande (20, 40, 80 ou 160MHz).

La plus part des AP actuels sont double-bande : 2,4GHz et 5GHz

WiFi generation	Date of release	Frequency band	Bandwidth	Maximum theoretical data rate	MIMO	Outdoor range
802.11a	1999	5	20 MHz	54 Mbit/s	No support	~110 m (5 GHz)
802.11b	1999	2.4 GHz	22 MHz	11 Mbit/s	No support	~130 m
802.11g	2003	2.4 GHz	22 MHz	54 Mbit/s	No support	~130 m
802.11n	2009	2.4 and 5 GHz	20 MHz, 40 MHz	Up to 600 Mbit/s (in 4x4 MIMO and 40 MHz bandwidth configuration)	Up to 4 x 4	~240 m
802.11ac	2012	5 GHz	20, 40, 80 or 160 MHz	Up to 6.77 Gbit/s (in 8 x 8 MIMO and 160 MHz bandwidth configuration)	Up to 8 x 8	

Source: IDATE





## IV.6/ Architectures Wi-Fi

Il y a deux architectures (topologies) principales :

- Ad hoc
- Infrastructure

### *IV.6.1/ Mode AD hoc*

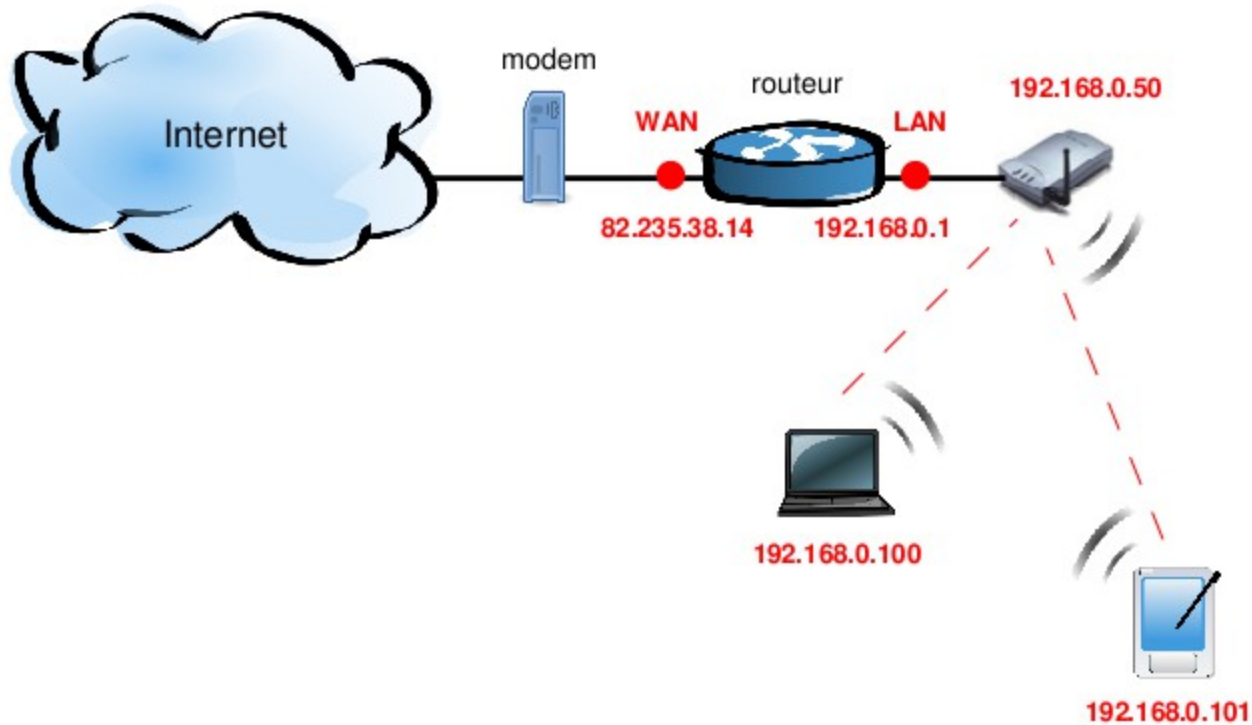
Avec deux ordinateurs ou plus équipés d'adaptateurs sans fil (cartes WiFi), il est possible de les relier très simplement en réseau en mettant en place un réseau dit « ad hoc », c'est-à-dire un réseau d'égal à égal, sans utiliser de point d'accès.

Si un des ordinateurs du réseau ad hoc possède une connexion à internet, il est alors possible de la partager avec les autres ordinateurs du réseau.



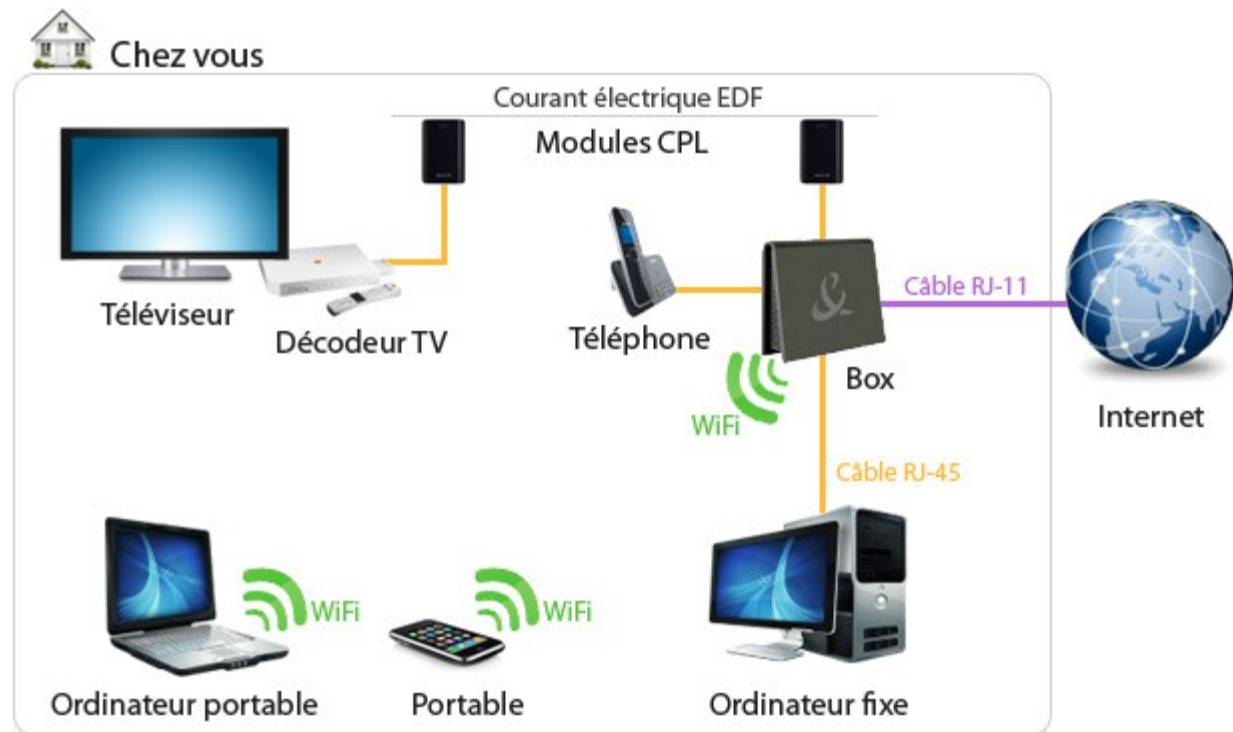
## IV.6.2/ Le mode infrastructure

Dans ce mode là un équipement particulier du réseau joue le rôle de point d'accès (AP)



### IV.6.3/ Un point d'accès Wi-Fi : la BOX

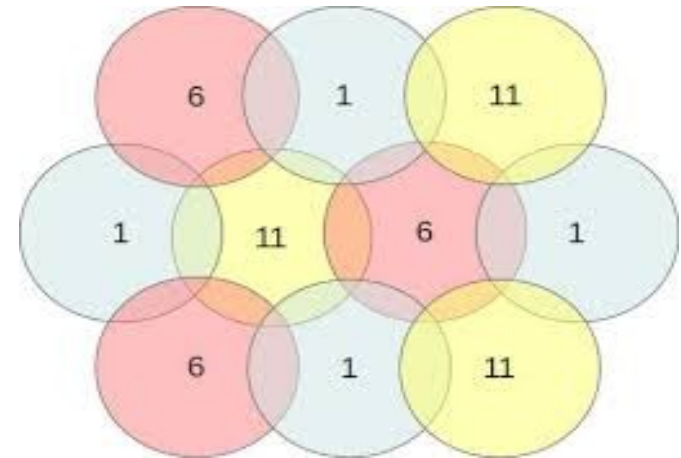
La Box joue ici, entre autres, le rôle de point d'accès Wi-Fi de routeur et de modem ADSL.



## IV.7/ Assurer une couverture à un site avec plusieurs AP

Si l'on souhaite obtenir une couverture convenable sur un site donné, il sera probablement nécessaire de placer plusieurs points d'accès. Dans un tel cas, les zones de couverture de plusieurs points d'accès viendront probablement se recouvrir partiellement. Il faudra donc choisir les canaux de chaque AP correctement!

- Comme nous l'avons vu précédemment les canaux 1, 6 et 11 ne se chevauchent pas !
- La zone ci-contre pourra être couverte par ces 10 AP configurés de cette façon



## IV.8/ Réglage d'un AP : exemple d'une BOX

Réseau local / Wi-Fi

État Wi-Fi Configuration Filtrage MAC FreeWifi

Carte Wi-Fi

Activer le réseau sans-fil : ☒

Canal : 12

Mode 802.11n : 20 Mhz

Réseau personnel

Activer le réseau personnel : ☒

Cacher le SSID : ☐

SSID : FreeboxRevolution

Type de protection : WPA-PSK

Clé Wi-Fi : zero-plus-zero=La-tete-a-toto

Filtrage d'adresse MAC : Liste blanche

Version du protocole EAPOL : Version 2

Restaurer les valeurs d'usine

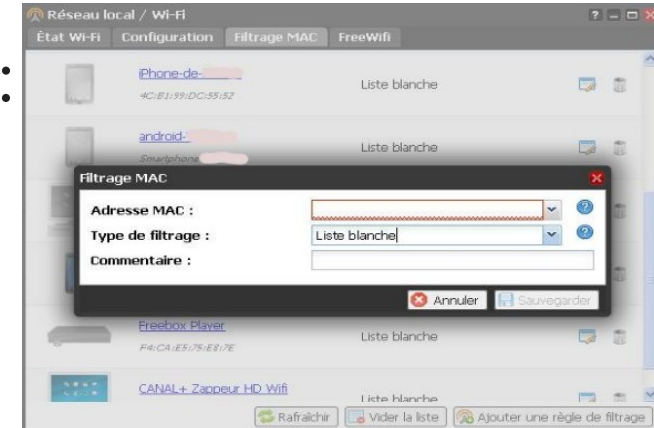
OK Annuler Appliquer

- Choix du canal (est il correct?)
- 20MHz ou 40MHz
- SSID : nom de l'AP (on peut le cacher)

- WPA : Wi-Fi Protected Acces : cryptage des données échangées entre l'AP et l'hôte
- WPA-PSK : mode personnel, pas de serveur d'authentification
- Clé Wi-Fi : phrase secrète partagée avec les stations
- Filtrage d'adresse MAC : on autorise seulement les stations définies dans une liste blanche à se connecter à l'AP

## IV.9/ Politique de sécurité

Restriction d'accès sur la base d'@ MAC:  
Établir une "liste blanche" de stations autorisées à se connecter



- Cacher le SSID : Votre AP n'apparaît plus dans la liste des réseaux disponibles !  
Peu efficace car on peut quand même le retrouver avec des logiciels spécialisés (type airodump, aircrack-ng, netstumbler...)
- Filtrage d'adresse MAC : les stations autorisées à se connecter ont été déclarées  
Peu efficace car on peut usurper une adresse MAC autorisée
- Cryptage WPA ou WPA2 : obligatoire
  - Attention à choisir une clé compliquée et la changer si nécessaire

# V/ La technologie CPL

## V.1/ Présentation

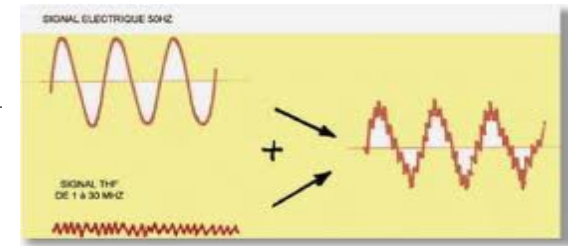
**La communication par Courants Porteurs en Ligne (CPL, PLC) utilise le réseau électrique existant pour transmettre des informations numériques.**

Le courant porteur haut débit résidentiel, dit «**Indoor**», est utilisé sur le réseau électrique privé de l'abonné, et permet la mise en place d'un réseau informatique local (LAN) personnel ou professionnel.

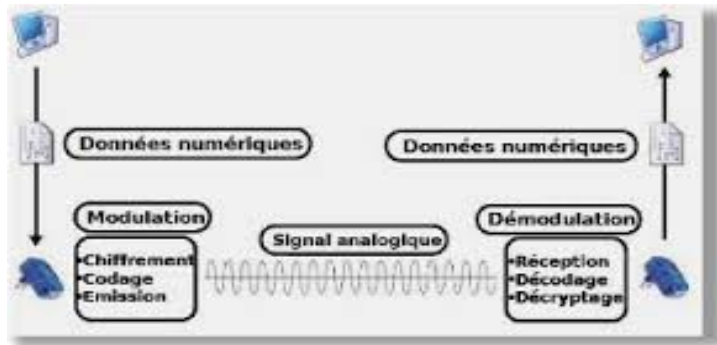
En «**Outdoor**» le courant porteur en ligne profite de l'infrastructure électrique moyenne et basse tension publique pour desservir un accès haut débit à Internet ou offrir d'autres applications distantes.

## V.2/ Fonctionnement

Le principe des CPL consiste à superposer au courant électrique alternatif de 50 Hz un signal à plus haute fréquence et de faible énergie (1 à 30MHz).



Ce signal se propage sur l'installation électrique et peut être reçu et décodé à distance par tout récepteur CPL de même catégorie se trouvant sur le même réseau électrique.





## V.3/ Exemple d'utilisation et caractéristiques

Dans un réseau domestique le CPL sert principalement à étendre la taille du réseau (Free et Orange livrent des plug CPL avec leurs BOX)!

Il est très fréquent de retrouver sur un même réseau domestique les technologies d'Ethernet filaire, WI-FI et CPL !

Les débits atteints sont compris entre 14 Mbit/s et 500 Mbps pour les normes HomePlug ou HomePlug AV.

Attention ces débits sont théoriques, le réseau électrique représentant en plus un HUB la bande passante est partagée (méthode d'accès CSMA-CA)!

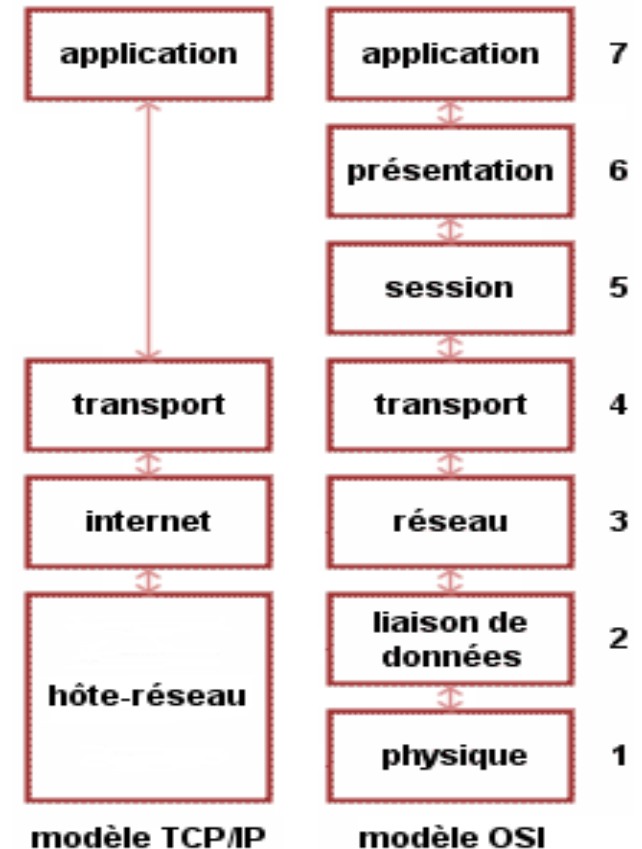
**Attention** : le réseau électrique n'est pas adapté au transport de signal haute-fréquence car il n'est pas blindé. En conséquence, la plus grande partie de l'énergie injectée par l'adaptateur CPL est rayonnée sous forme d'onde radio.

# VI/ Les protocoles TCP/IP

## VI.1/ Présentation

Le modèle TCP/IP s'est progressivement imposé comme modèle de référence en lieu et place du modèle OSI.

- TCP et IP inventés en 1974
- Technologie de commutation par paquet (mode datagramme)
- Protocoles à la base de INTERNET



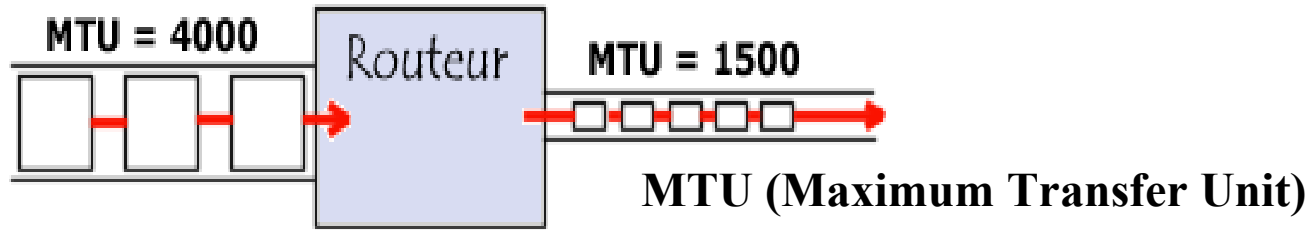
## VI.2/ Internet Protocol

Le concept d'interconnexion ou **d'*internet*** repose sur la mise en œuvre d'une couche réseau masquant les détails de la communication physique du réseau et détachant les applications des problèmes de routage.

L'interconnexion : faire transiter des informations depuis un réseau vers un autre réseau par des nœuds spécialisés appelés passerelles (*gateway*) ou routeurs (*router*)

Le routage des paquets est effectué de proche en proche (un routeur ne connaît pas la route complète).

- Elaboration des paquets (éventuellement segmentation de ceux-ci):



- Routage des paquets jusqu'à la machine destinataire
- Mécanisme d'adressage permettant d'identifier un réseau et une machine sur ce réseau

- **Assurer un service fiable:**

IP ne vérifie pas que les paquets sont bien arrivés.

- **Etablir une liaison de bout en bout, un mode connecté:**

Les paquets ne suivent pas tous forcément le même chemin!

Il n'est pas garanti qu'ils arrivent dans l'ordre d'émission!

### Introduction

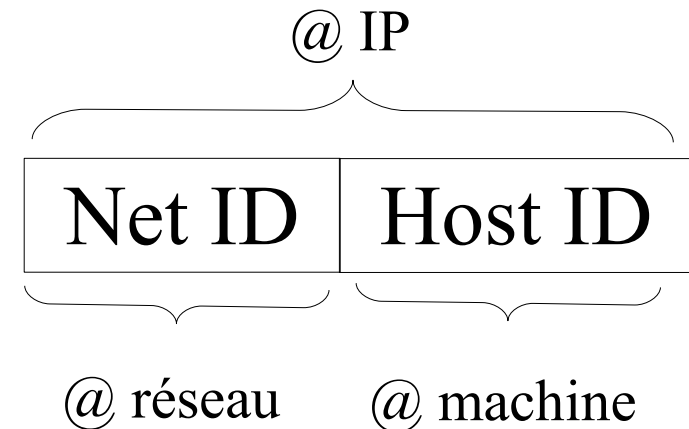
Une adresse IPV4 est formée de 4 octets:

**ex:** 1100 0011 1000 1001 0010 0000 0001 0111 est une adresse IP  
Pour plus de lisibilité on utilise la notation décimale pointée:  
**195.137.32.23**

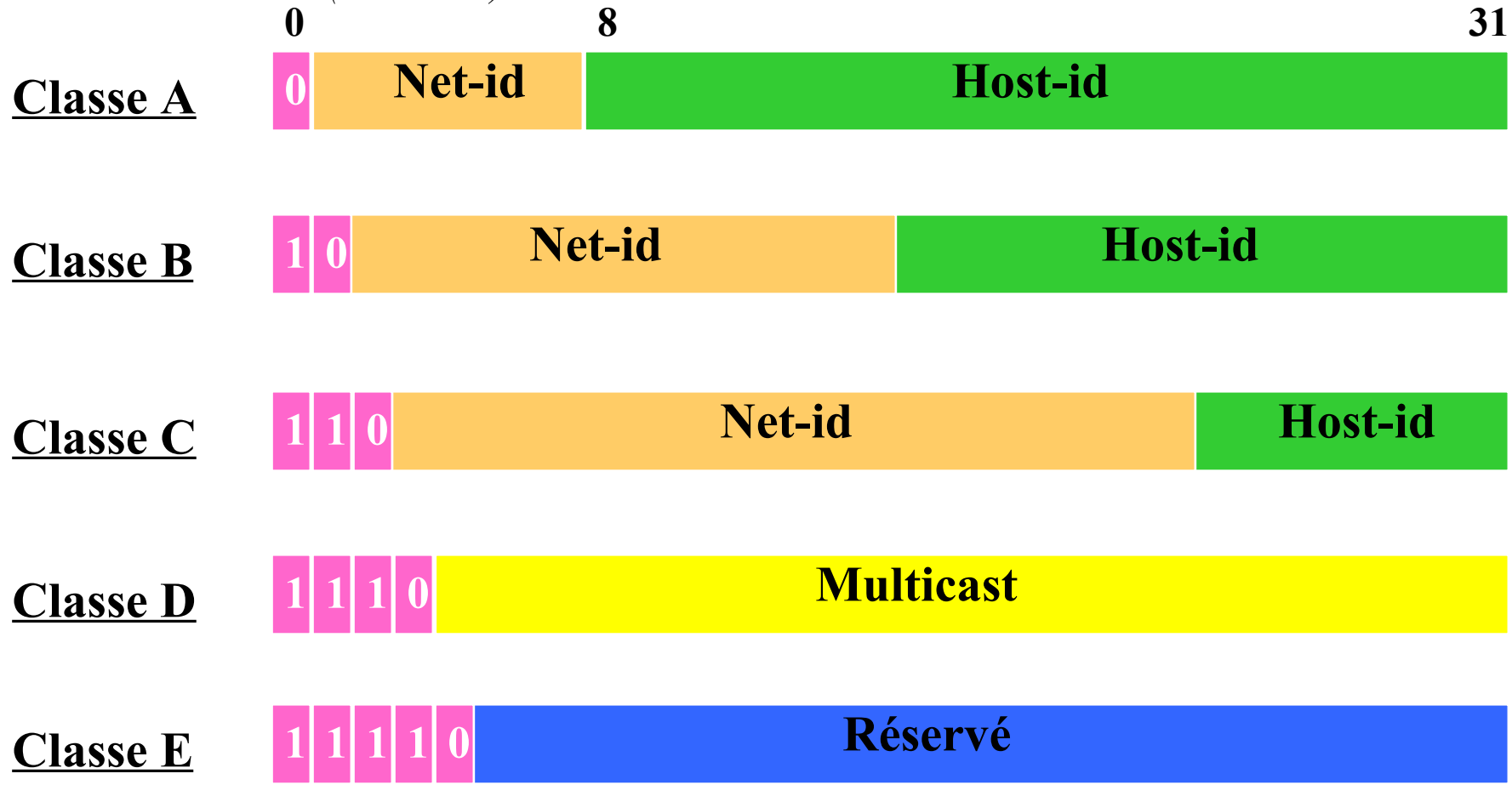
Elle permet d'identifier un réseau dans le monde et une machine dans ce réseau.

**La taille du Net ID et du host ID dépendent de la classe d'adressage.**

**Cette notion de classe d'adresse est obsolète mais aide à comprendre l'adressage IP.**



Les classes d'adresse (obsolète)



Masque par défaut associé à la classe :

Classe A : 255.0.0.0

Classe B : 255.255.0.0

Classe C : 255.255.255.0

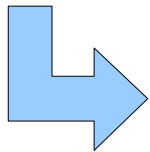
- ✓ Réseaux de classe A: 1.0.0.0 à 127.0.0.0 avec 16 777 214 machines max
- ✓ Réseaux de classe B: 128.0.0.0 à 191.255.0.0 avec 65534 machine max
- ✓ Réseaux de classe C: 192.0.0.0 à 223.255.255.0 avec 254 machines max

✗ Si tous les bits du Host-Id à 1: le datagramme est adressé à toutes les machines du réseau: ➡ **diffusion**

✗ Si tous les bits du Host-Id à 0: il s'agit de l'adresse du réseau

Il existe aussi un masque de sous réseau (net mask) composé de 4 octets. Il permet de distinguer le Host id et le Net id dans l'adresse.

<b>Règles:</b>	<b>Adresse IP</b>	<b>Adresse IP</b>
	<b>&amp; Net Mask</b>	<b>  NOT (Net Mask)</b>
	<b>Adresse du réseau</b>	<b>Adresse de diffusion</b>



**Permet de créer des sous réseaux: subnetting**  
**Permet de faire abstraction des classes d'adresse**



## VI.2.4/ Principe de subnetting avec masque de taille fixe

Il s'agit de partitionner un réseau en plusieurs sous réseaux  
Certains bits de la partie HostId sont utilisés comme SubnetId

### Exemple sur un réseau de classe C:

Masque par défaut

255.255.255.0 (11111111.11111111.11111111.00000000 binary)

Nouveau masque:

255.255.255.240 (11111111.11111111.11111111.11110000 binary)

Possibilité de créer  $2^4 - 2 = 14$  sous réseaux

# bits	Subnet Mask	CIDR	# Subnets	# Hosts	Nets * Hosts
2	255.255.255.192	/26	2	62	124
3	255.255.255.224	/27	6	30	180
4	255.255.255.240	/28	14	14	196
5	255.255.255.248	/29	30	6	180
6	255.255.255.252	/30	62	2	124

## VI.2.5/ Évolutions de l'adressage IPV4

### **Historique** : Optimisation de l'espace d'adresse IPV4 (pénurie)

Le VLSM & la notation CIDR (1993, RFC 1519)

=> adressage classless, la classe d'adresse n'a plus de sens !

- NAT (Network Address Translation) (1994, RFC 1631)
- Adressage privé (1996, RFC 1918)

*A/ La notation CIDR* : Vu que la classe d'adresse n'a plus de sens, chaque adresse est associée à un masque spécifique

### **Caractéristique des masques de sous réseau :**

« *Les bits à 1 ne se mélangent pas avec les bits à 0* », en effet dans un masque correct les 1 sont à gauche et les 0 à droite :

255.255.255.0 (11111111.11111111.11111111.00000000 binary)

255.255.255.192 (11111111.11111111.11111111.11000000 binary)

~~255.255.255.64 (11111111.11111111.11111111.01000000 binary)~~

### **Conséquence:**

Pour identifier un masque il suffit de connaître le nombre de bits à 1 qui le compose.

### **Principe de la notation CIDR :**

C'est l'adresse IP suivie d'un (slash) / et du nombre de bits à 1 du masque

Notation CIDR	Notation Standard
192.168.1.15/24	192.168.1.15 mask :255.255.255.0
212.36.17.163/26	212.36.17.163 mask : 255.255.255.192
10.3.54.21/29	10.3.54.21 mask : 255.255.255.248
176.31.25.46/16	176.31.25.46 mask : 255.255.0.0

## ***B/ Le subnetting en taille de masque variable (VLSM)***

**Principe** : La taille du masque est variable et adaptée à la taille du sous réseau.

**Exemple** : Soit le réseau 192.168.1.0/24 devant être partitionné en :  
Lan1 : 97 machines, lan2 : 12 machines, Lan3: 2 machines

Réseau	Hôtes	CIDR	Masque	@Sous_réseau	@Diffusion
Lan1	97	/25	255.255.255.128	192.168.1.0	192.168.1.127
Lan2	12	/28	255.255.255.240	192.168.1.128	192.168.1.143
Lan3	2	/30	255.255.255.254	192.168.1.252	192.168.1.255

### *Explications :*

Pour un réseau avec 97 machines il faut 99 adresses soit un hostid de 7 bits ( $2^7 = 128$ )

Donc le masque sera 32-7 soit 25

Pour un réseau avec 12 machines il faut 14 adresses soit un hostid de 4 bits ( $2^4 = 16$ )

Donc le masque sera 32-4 soit 28

Pour un réseau avec 2 machines il faut 4 adresses soit un hostid de 2 bits ( $2^2 = 4$ )

Donc le masque sera 32-2 soit 30

Il faut faire attention que les différents réseaux ne se chevauchent pas et appartiennent tous (c-a-d soient inclus) au réseau 192.168.1.0/24

### *C/ L'adressage privé*

Une adresse privée n'est pas routée sur Internet !

Ce type d'adresse est utilisé dans des réseaux privés (domicile, entreprises, campus, base militaires...), pour « aller » sur Internet à partir de ces réseaux il sera nécessaire de faire une translation d'adresse.

En IPv4, les classes d'adresses ont été réservées comme suit (cf. RFC 1918)

10.0.0.1 à 10.255.255.254 (notation CIDR : 10.0.0.0/8)

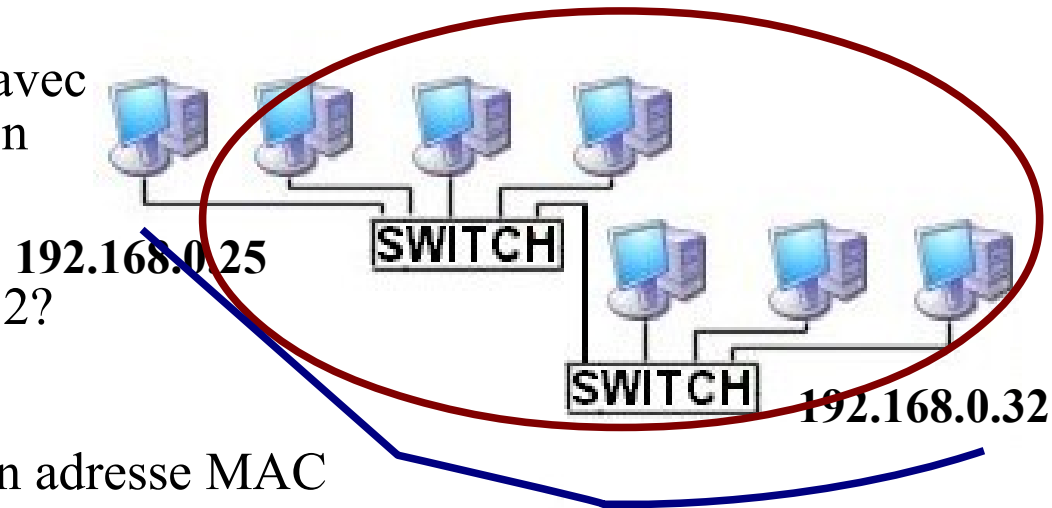
172.16.0.1 à 172.31.255.254 (notation CIDR : 172.16.0.0/12)

192.168.0.1 à 192.168.255.254 (notation CIDR : 192.168.0.0/16)

## VI.2.7/ Le protocole ARP

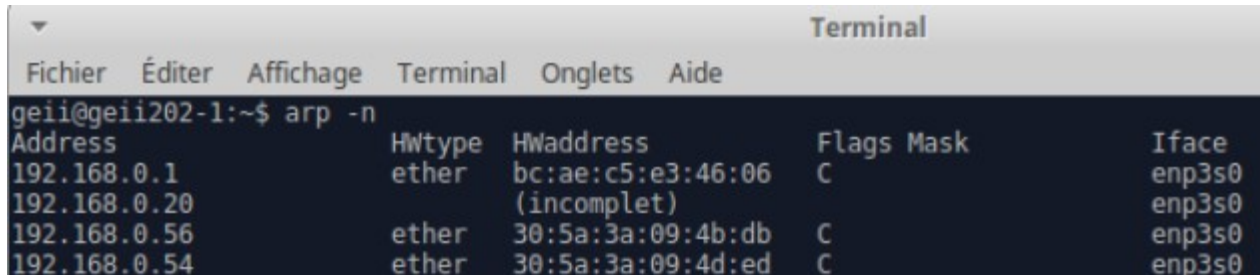
L'Address resolution protocol (ARP, protocole de résolution d'adresse) effectue la traduction d'une adresse IP en une adresse ethernet (adresse MAC). Ce protocole est distinct de IP, de même niveau (3) et invoqué par lui.

- 192.168.0.25 tente de communiquer avec 192.168.0.32, mais ne connaît pas son adresse MAC
- Diffusion: qui a l'adresse 192.168.0.32?
- 192.168.0.32 réponds en donnant son adresse MAC
- 192.168.0.25 conserve quelques temps l'adresse MAC de 192.168.0.32 dans sa table des entrées arp



## VI.2.7/ Le protocole ARP (suite)

Pour visualiser la table des entrées ARP on utilise la commande *arp -n*



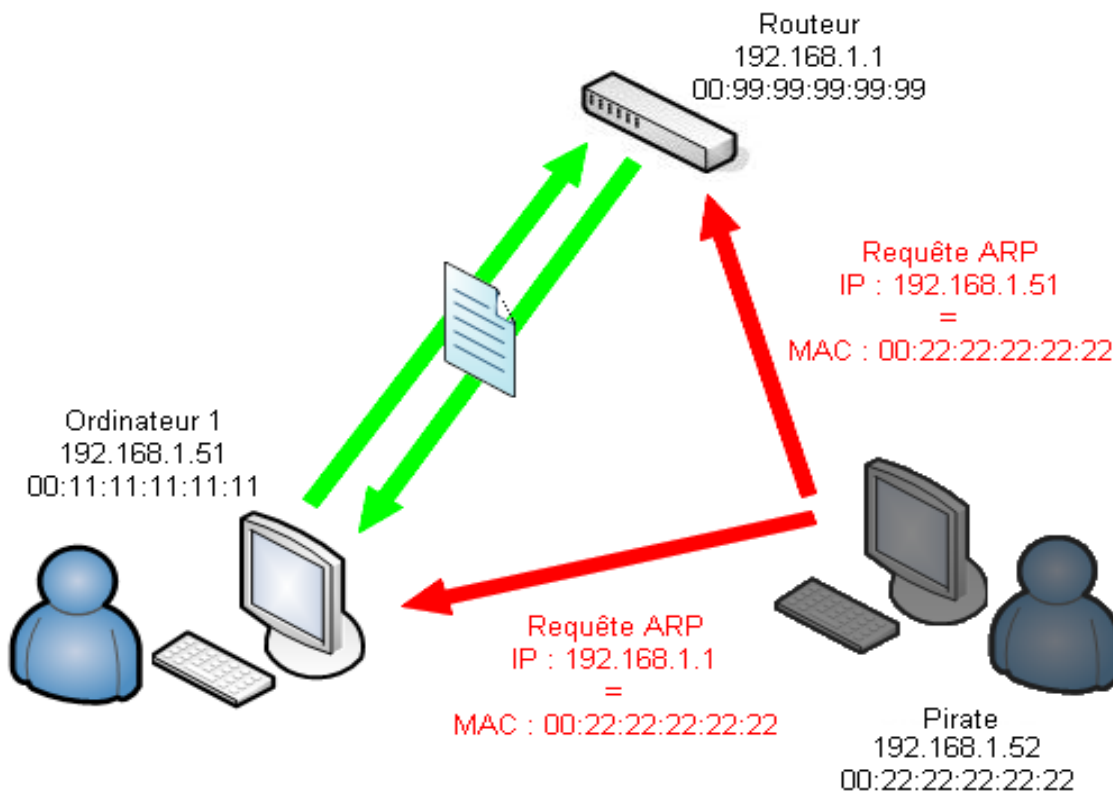
```
geii@geii202-1:~$ arp -n
Address                  Hwtype  Hwaddress      Flags  Mask    Iface
192.168.0.1              ether   bc:ae:c5:e3:46:06  C        
192.168.0.20             ether   (incomplet)      C      enp3s0
192.168.0.56             ether   30:5a:3a:09:4b:db  C      enp3s0
192.168.0.54             ether   30:5a:3a:09:4d:ed  C      enp3s0
```

Cela nous permet entre autre de savoir avec quelles machines notre ordinateur à communiqué récemment

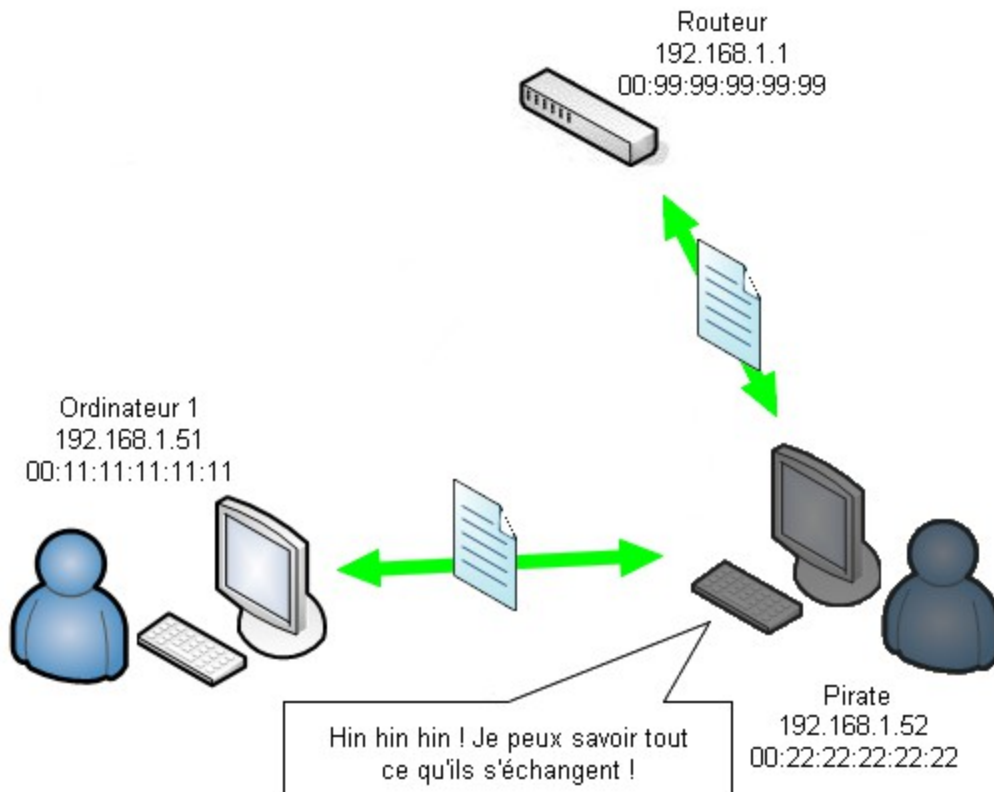
ARP spoofing (ou ARP poisoning) :

Cette technique utilise une faille du protocole ARP qui consiste à se déclarer sur un réseau en émettant (broadcast) un paquet ARP faux (ex gratuitous arp avec une adresse IP qui n'est pas la notre). Dans ce cas il est possible d'associer notre adresse MAC à l'adresse IP d'une autre machine dont on souhaite intercepter les communications.

C'est la base de l'attaque de « l'homme du milieu » (MITM).



Les réseaux de zéro - [siteduzero.com](http://siteduzero.com)

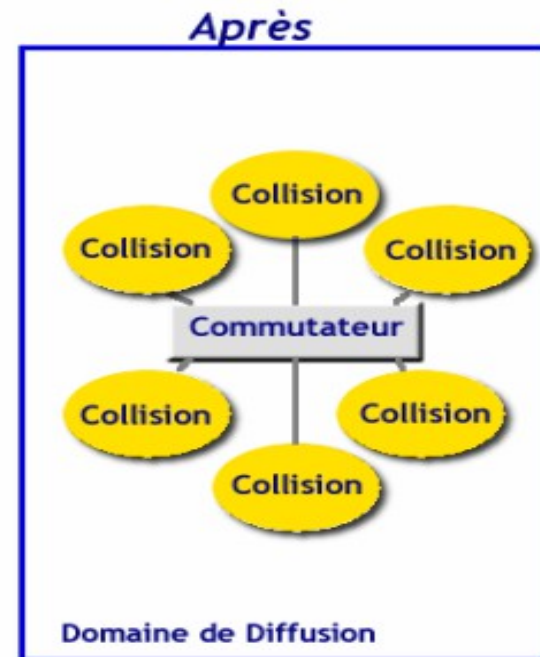


Les réseaux de zéro - siteduzero.com



## Un commutateur segmente des domaines de collision

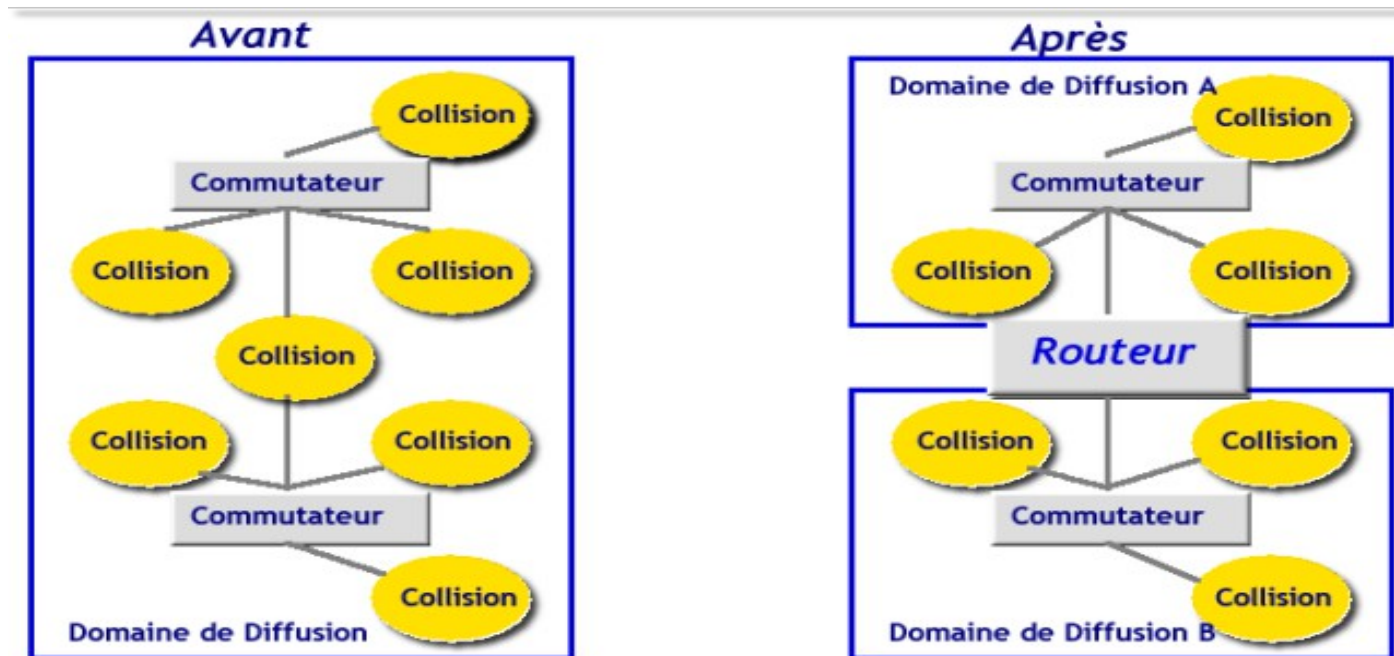
La segmentation au niveau 2 réduit le nombre de stations en compétition sur le même réseau local. Chaque domaine de collision possède la bande passante délivrée par le port du commutateur.



**NB :** Un commutateur (switch) transmet la trame à la (aux) machine(s) destinataires!

# Un routeur segmente des domaines de diffusion

La segmentation au niveau 3 réduit le trafic de diffusion en divisant le réseau en sous-réseaux indépendants.



**NB :** un routeur ne retransmets pas une diffusion!

## VI.2.9/ L'en tête IP V4

←-- 32 bits

Version (4 bits)	Longueur d'en-tête (4 bits)	Type de service (8 bits)	Longueur totale (16 bits)	
Identification (16 bits)			Drapeau (3 bits)	Décalage fragment (13 bits)
Durée de vie (8 bits)		Protocole (8 bits)	Somme de contrôle en-tête (16 bits)	
Adresse IP source (32 bits)				
Adresse IP destination (32 bits)				
Données				

- Version:
- Longueur:
- Identification:
- Durée de vie:
- Somme de contrôle:
- Adresse IP source :
- Adresse IP dest :
- ...

## VI.3/ Transport Control Protocol

**TCP permet d'établir une connexion fiable et sans erreur.**

**Les caractéristiques principales du protocole TCP sont les suivantes:**

- \* TCP permet de remettre en ordre les datagrammes en provenance du protocole IP
- \* TCP permet de vérifier le flot de données afin d'éviter une saturation du réseau
- \* TCP permet de multiplexer les données, c'est-à-dire de faire circuler simultanément des informations provenant de sources (applications par exemple) distinctes sur une même ligne
- \* TCP permet l'initialisation et la fin d'une communication, c'est un mode connecté

## VI.3.1/ L'en tête TCP

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Port Source																Port destination															
Numéro d'ordre																															
Numéro d'accusé de réception																															
Décalage données		réservée		URG	ACK	PSH	RST	SYN	FIN	Fenêtre																					
Somme de contrôle																Pointeur d'urgence															
Options																						Remplissage									
Données																															

Un numéro de port identifie un processus (une application) .

## VI.4/ L'encapsulation des données

Données

En tête TCP    Données

En tête IP    En tête TCP    Données

Données de la couche 3

En tête Ethernet    En tête IP    En tête TCP    Données    CRC Ethernet

Données de la couche 2

# L'encapsulation des données, analyse de trame

Trame envoyée

0000	00	0b	6a	9e	cb	cf	00	50	da	06	82	83	08	00	45	00	..j....P.....E.
0010	00	69	f4	b6	40	00	40	06	c4	4c	c0	a8	00	01	c0	a8	.i..@.@. .L.....
0020	00	3a	0c	38	04	40	4a	ca	36	b0	1c	e9	a6	9d	50	18	..8.@J. 6.....P.
0030	19	20	96	66	00	00	5a	2e	d7	bc	c0	01	8b	f2	07	bf	. .f..Z. ....
0040	18	55	43	41	79	ce	74	87	5c	77	6f	c6	02	71	6d	22	.UCAy.t. \wo..qm"
0050	2d	22	59	a7	74	ea	12	02	37	e7	d5	fe	d5	51	cf	50	-"Y.t... 7....Q.P
0060	bf	ac	17	c2	e4	62	61	a2	4f	63	b0	14	ef	63	9f	d3	.....ba. Oc...C..
0070	52	f8	6a	0f	d8	39	1c										R.j..9.

En tête Ethernet

0000	00	0b	6a	9e	cb	cf	00	50	da	06	82	83	08	00	45	00	..j....P.....E.
0010	00	69	f4	b6	40	00	40	06	c4	4c	c0	a8	00	01	c0	a8	.i..@.@. .L.....
0020	00	3a	0c	38	04	40	4a	ca	36	b0	1c	e9	a6	9d	50	18	..8.@J. 6.....P.
0030	19	20	96	66	00	00	5a	2e	d7	bc	c0	01	8b	f2	07	bf	. .f..Z. ....
0040	18	55	43	41	79	ce	74	87	5c	77	6f	c6	02	71	6d	22	.UCAy.t. \wo..qm"
0050	2d	22	59	a7	74	ea	12	02	37	e7	d5	fe	d5	51	cf	50	-"Y.t... 7....Q.P
0060	bf	ac	17	c2	e4	62	61	a2	4f	63	b0	14	ef	63	9f	d3	.....ba. Oc...C..
0070	52	f8	6a	0f	d8	39	1c										R.j..9.

En tête IP

0000	00	0b	6a	9e	cb	cf	00	50	da	06	82	83	08	00	45	00	..j....P.....E.
0010	00	69	f4	b6	40	00	40	06	c4	4c	c0	a8	00	01	c0	a8	.i..@.@. .L.....
0020	00	3a	0c	38	04	40	4a	ca	36	b0	1c	e9	a6	9d	50	18	..8.@J. 6.....P.
0030	19	20	96	66	00	00	5a	2e	d7	bc	c0	01	8b	f2	07	bf	. .f..Z. ....
0040	18	55	43	41	79	ce	74	87	5c	77	6f	c6	02	71	6d	22	.UCAy.t. \wo..qm"
0050	2d	22	59	a7	74	ea	12	02	37	e7	d5	fe	d5	51	cf	50	-"Y.t... 7....Q.P
0060	bf	ac	17	c2	e4	62	61	a2	4f	63	b0	14	ef	63	9f	d3	.....ba. Oc...C..
0070	52	f8	6a	0f	d8	39	1c										R.j..9.

## En tête TCP

0000	00 0b 6a 9e cb cf 00 50 da 06 82 83 08 00 45 00	..j....P .....E.
0010	00 69 f4 b6 40 00 40 06 c4 4c c0 a8 00 01 c0 a8	.i...@.@. .L.....
0020	00 3a 0c 38 04 40 4a ca 36 b0 1c e9 a6 9d 50 18	...8.@J. 6.....P.
0030	19 20 96 66 00 00 5a 2e d7 bc c0 01 8b f2 07 bf	. .f..Z. ....
0040	18 55 43 41 79 ce 74 87 5c 77 6f c6 02 71 6d 22	.UCAy.t. \wo..qm"
0050	2d 22 59 a7 74 ea 12 02 37 e7 d5 fe d5 51 cf 50	-"Y.t... 7....Q.P
0060	bf ac 17 c2 e4 62 61 a2 4f 63 b0 14 ef 63 9f d3	.....ba. Oc...C..
0070	52 f8 6a 0f d8 39 1c	R.j..9.

## Données

0000	00 0b 6a 9e cb cf 00 50 da 06 82 83 08 00 45 00	..j....P .....E.
0010	00 69 f4 b6 40 00 40 06 c4 4c c0 a8 00 01 c0 a8	.i...@.@. .L.....
0020	00 3a 0c 38 04 40 4a ca 36 b0 1c e9 a6 9d 50 18	...8.@J. 6.....P.
0030	19 20 96 66 00 00 5a 2e d7 bc c0 01 8b f2 07 bf	. .f..Z. ....
0040	18 55 43 41 79 ce 74 87 5c 77 6f c6 02 71 6d 22	.UCAy.t. \wo..qm"
0050	2d 22 59 a7 74 ea 12 02 37 e7 d5 fe d5 51 cf 50	-"Y.t... 7....Q.P
0060	bf ac 17 c2 e4 62 61 a2 4f 63 b0 14 ef 63 9f d3	.....ba. Oc...C..
0070	52 f8 6a 0f d8 39 1c	R.j..9.



## VI.5/ Le modèle client serveur

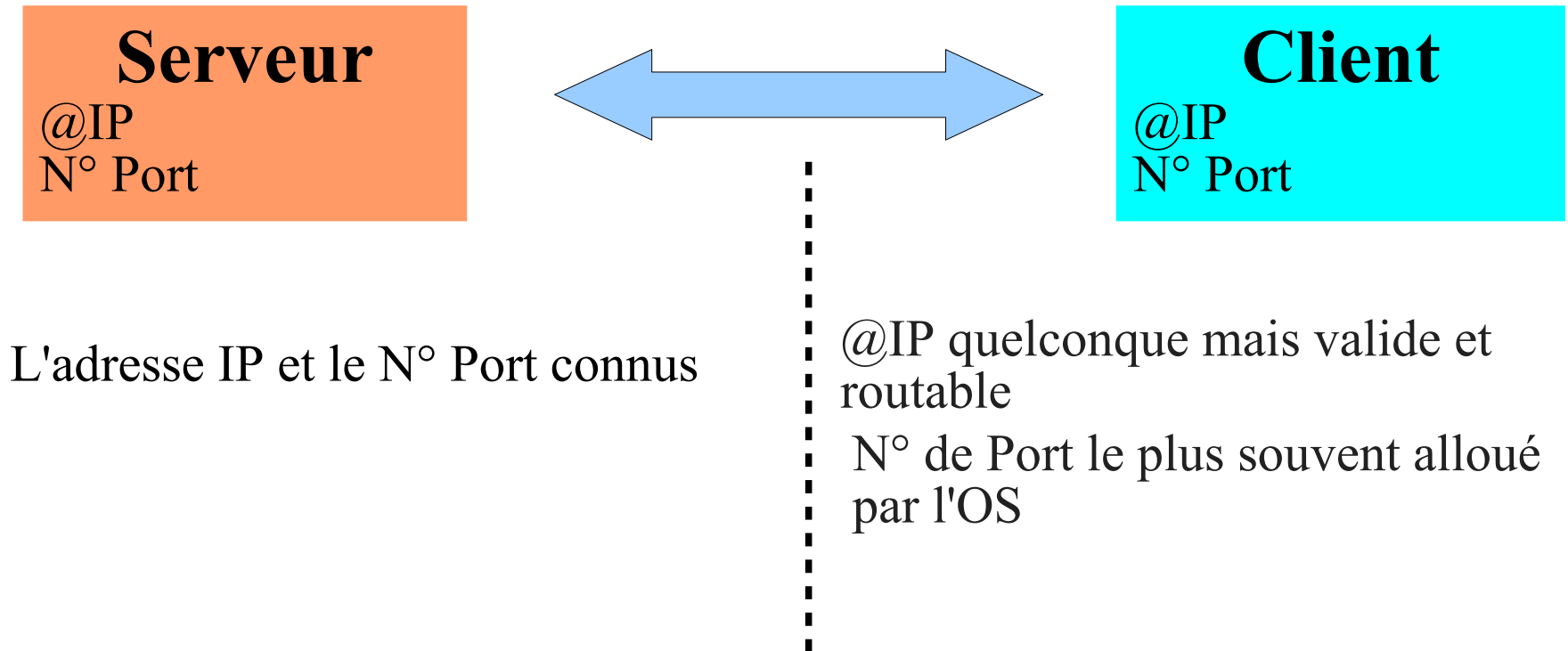
Un serveur est une application, repérée par un numéro de **port**, à laquelle il est possible de se connecter pour échanger des informations.

Il est aussi nécessaire de connaître l'adresse (IP ou nom DNS) de la machine qui héberge cette application.

En se connectant, un client, qui est aussi une application repérée par un numéro de **port**, utilise ce service.

Le client s'exécute sur une machine identifiée par une adresse IP.

**Connexion à l'initiative du client**  
puis communication bidirectionnelle suivant  
protocole (couches 5,6&7 du modèle OSI)



## Le modèle client serveur (exemple)

APACHE  
HTTP SERVER



Serveur WEB



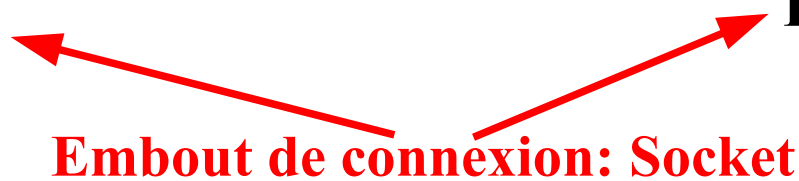
Client WEB

**72.14.221.79 ( [www.google.fr](http://www.google.fr) )**  
**Port 80 (http)**  
**TCP**



**195.138.62.23**  
**Port 1235**  
**TCP**

**Embout de connexion: Socket**



## Quelques ports connus

<b>Port</b>	<b>Service ou Application</b>
21	FTP
22	SSH
23	Telnet
25	SMTP
53	Domain Name System
63	Whois
70	Gopher
79	Finger
80	HTTP
110	POP3
119	NNTP

## **Système embarqué:**

Client ou serveur pour applications «propriétaires»

Intègre un serveur WEB « enfouis »

Envoi d'email sur alarme...

INTRANET  
ou  
INTERNET



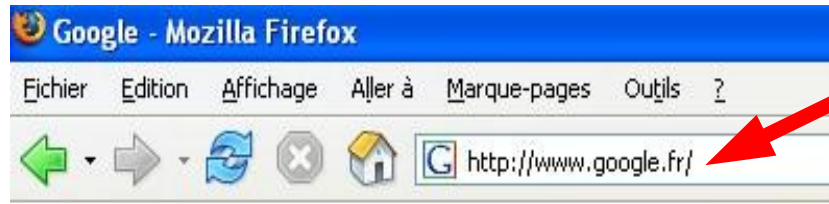
# VII/ Quelques applications

## VII.1/ DNS (Domain Name system)



Il est plus facile de retenir une adresse textuelle que numérique!  
74.14.221.104 ou [www.google.fr](http://www.google.fr) !

**Le DNS permet de faire la résolution de nom de domaine ou d'adresse, c-a-d de déterminer l'un en fonction de l'autre.**



Automatiquement le serveur de noms est interrogé pour obtenir l'@IP de google

Sous *Windows et linux*, l'utilitaire *nslookup* permet d'interroger le serveur de nom.

```
stephane@stephane-PC-Fixe:~$ nslookup meteo.fr
Server:      127.0.0.53
Address:     127.0.0.53#53
```

← Demande au serveur DNS par défaut

```
Non-authoritative answer:
Name:   meteo.fr
Address: 137.129.43.129
```

← Réponse IPV4

```
stephane@stephane-PC-Fixe:~$ nslookup www.google.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53
```

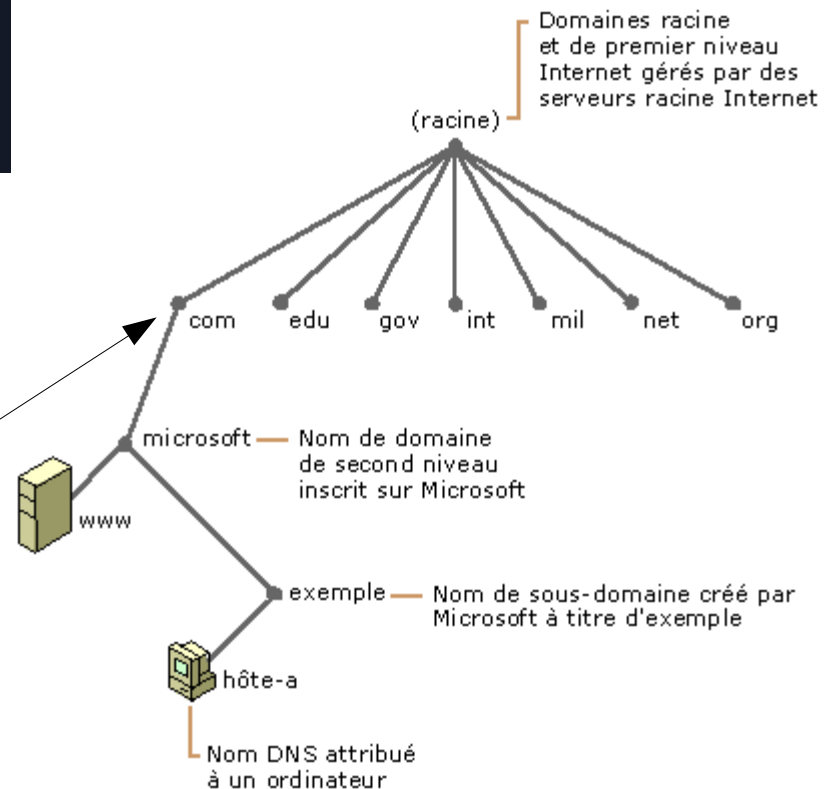
← Serveur de nom 8.8.8.8

```
Non-authoritative answer:
Name:   www.google.com
Address: 172.217.18.228
Name:   www.google.com
Address: 2a00:1450:4006:802::2004
```

```
stephane@stephane-PC-Fixe:~$ nslookup 8.8.8.8
8.8.8.8.in-addr.arpa    name = dns.google.
```

```
stephane@stephane-PC-Fixe:~$ nslookup 137.129.43.129
129.43.129.137.in-addr.arpa    name = www.meteo.fr.
```

(Top Level Domain)



## VII.2/ DHCP (Dynamic Host Control Protocol)

DHCP est un protocole qui permet à un système informatisé qui se connecte sur un réseau d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration IP qui est composée de:

- Adresse IP
- Masque
- Passerelle
- Serveur DNS

Le serveur DHCP possède lui une adresse IP fixe. Il délivre les configuration IP pour une durée déterminée: Bail.

**NB1** : Ne pas confondre adressage statique et adressage dynamique, dans le cas d'un adressage statique c'est l'administrateur du système qui renseigne la configuration IP.

La BOX INTERNET joue le rôle de serveur DHCP pour le réseau privé!

**NB2** : Dans le réseau de l'atelier GE, le serveur DHCP distribue des adresses de la forme 192.168.0.XX avec XX compris entre 20 et 80. Quelles sont les deux plages d'adresses statiques ?



## VII.3/ telnet

TERminal NETwork est un protocole permettant de se connecter sur une machine distante. Par défaut il utilise le port 23.

Telnet, n'étant pas un protocole sécurisé, a été abandonné au profit de SSH (Secure SHell).

On l'utilise encore souvent, non pas pour se connecter sur une machine distante, mais pour utiliser d'autres services sur d'autres ports.

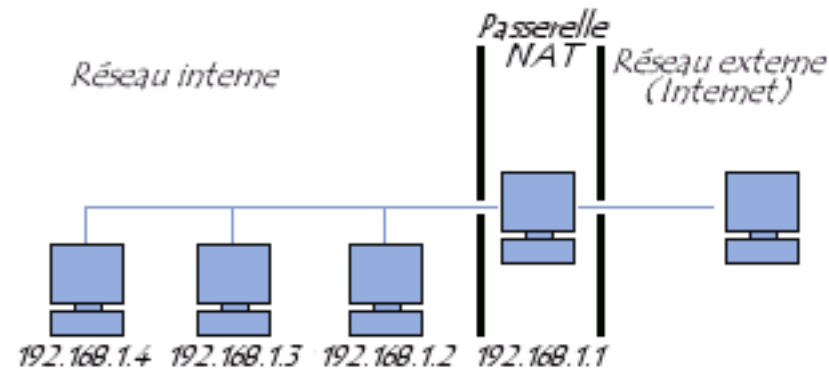
**telnet @machine port**

***telnet 192.168.0.1 3128***

Test du service proxy WEB (port 3128) de la passerelle de l'atelier GEII

## VII.4/ Network Address Translation (NAT)

Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP



Pour retrouver le destinataire des paquets entrants, la passerelle NAT utilise:

- ✓ L'IP source du paquet et/ou le protocole utilisé
- ✓ Le ports de destination (possibilité d'effectuer si nécessaire une translation de port : PAT).

La BOX Internet joue le rôle de passerelle NAT!



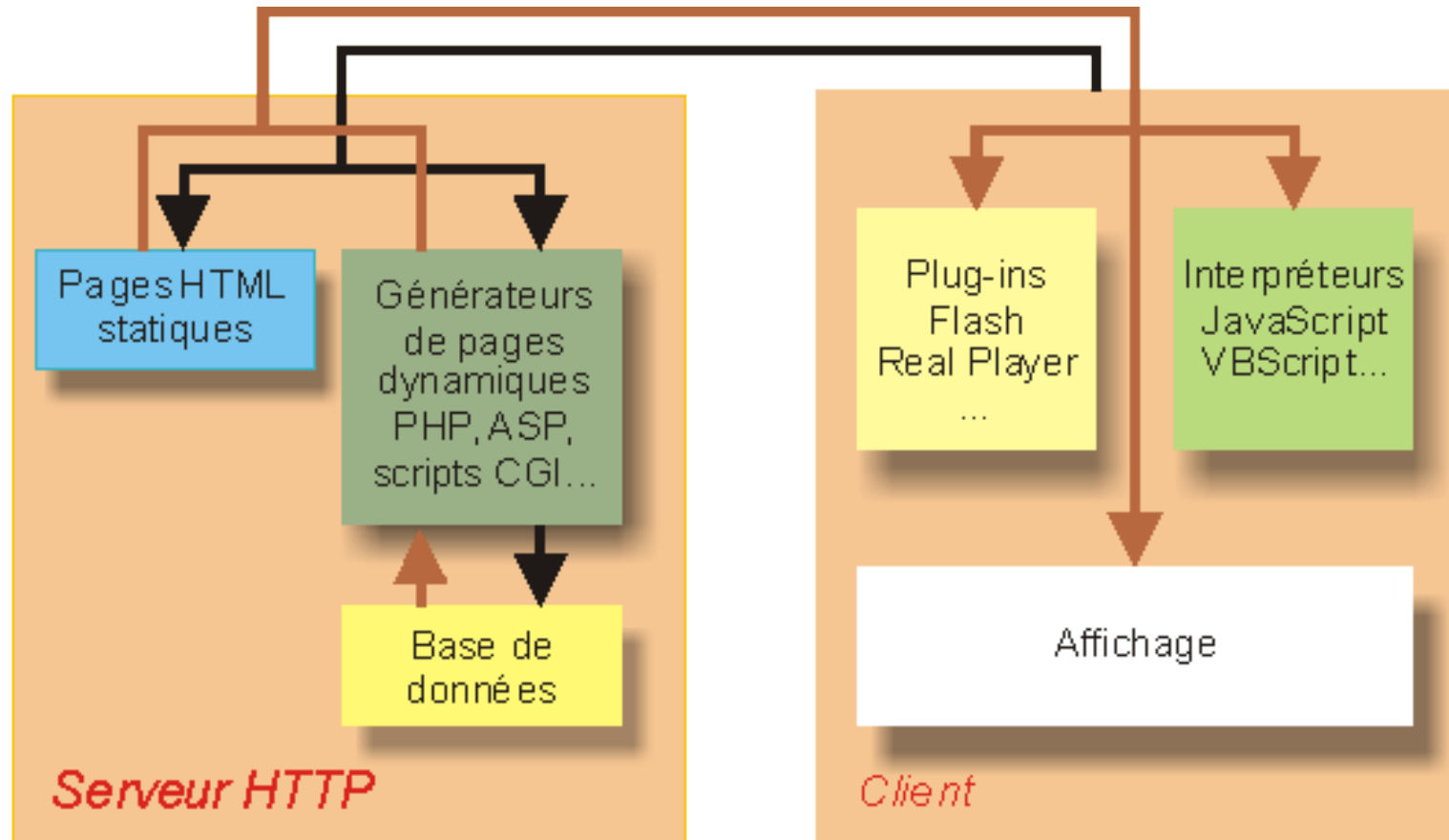
**Le Port Forwarding** permet à l'extérieur d'accéder à un service (serveur WEB ou autre) qui est en fait basé sur une machine du réseau privé .

La machine distante pense communiquer avec la machine hébergeant le NAT alors qu'en fait celui-ci redirige le flux vers la machine correspondant réellement à ce service.

Les adresses dites non-routables (privées) correspondent aux plages d'adresses suivantes :

- \* Classe A : plage de 10.0.0.0 à 10.255.255.255
- \* Classe B : plage de 172.16.0.0 à 172.31.255.255
- \* Classe C : plage de 192.168.0.0 à 192.168.255.55

## VII.5/ HTTP



# HTTP (capture de trame)

Source	Destination	Protocol	Info
192.168.1.13	193.49.96.35	TCP	47680 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=1344128 TSE
193.49.96.35	192.168.1.13	TCP	http > 47680 [SYN, ACK] Seq=0 Ack=1 Win=61440 Len=0 MSS=1460 WS=
192.168.1.13	193.49.96.35	TCP	47680 > http [ACK] Seq=1 Ack=1 Win=5888 Len=0
192.168.1.13	193.49.96.35	HTTP	GET / HTTP/1.1
193.49.96.35	192.168.1.13	TCP	http > 47680 [ACK] Seq=1 Ack=414 Win=61027 Len=0
193.49.96.35	192.168.1.13	HTTP	HTTP/1.1 200 OK (text/html)
192.168.1.13	193.49.96.35	TCP	47680 > http [ACK] Seq=414 Ack=1391 Win=8768 Len=0
192.168.1.13	193.49.96.35	TCP	47680 > http [FIN, ACK] Seq=414 Ack=1391 Win=8768 Len=0

## ▼ Hypertext Transfer Protocol

▶ GET / HTTP/1.1\r\n

Host: stephane.pignol.univ-tln.fr\r\n

User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.9.0.4) Gecko/2008111317 Ubuntu/8.04 (hardy) Firefox/3.0.4\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n

Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3\r\n

Accept-Encoding: gzip,deflate\r\n

Accept-Charset: ISO-8859-1,utf-8;q=0.7,\*;q=0.7\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

\r\n

## HTTP (Codes)

**Quelques codes utilisés avec HTTP :** **2XX Succès**  
**4XX Erreur client**  
**5XX Erreur serveur**

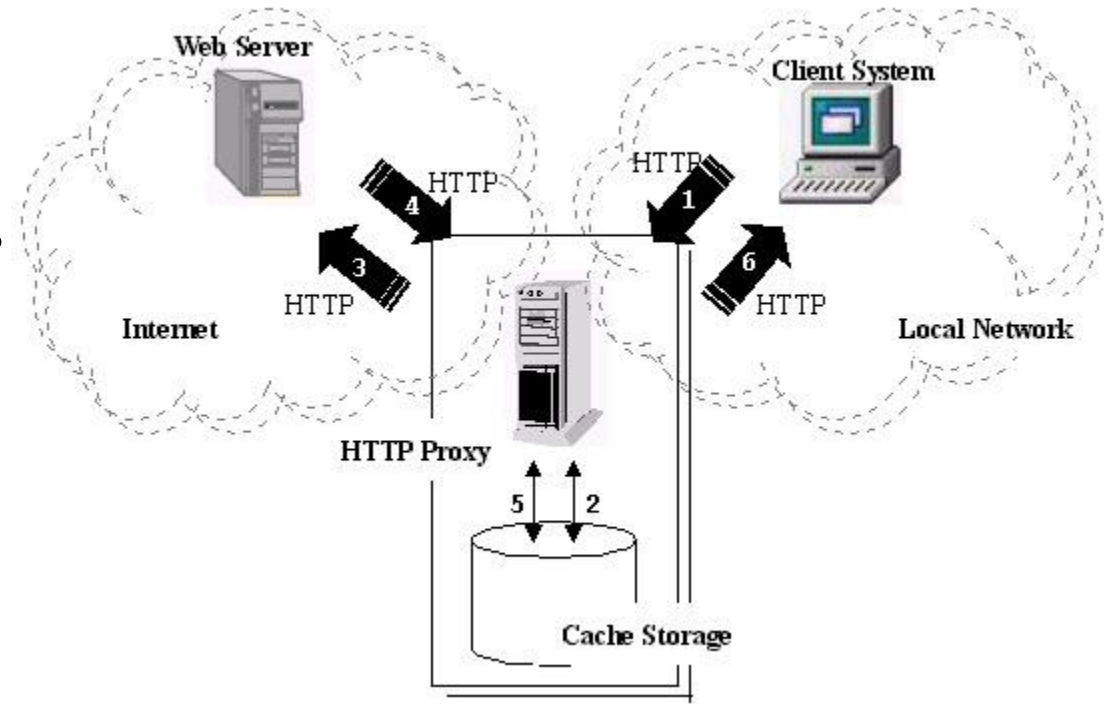
Code Message	Signification
<b>200 OK</b>	Requête traitée avec succès
<b>400 Bad Request</b>	La syntaxe de la requête est erronée
<b>401 Unauthorized</b>	Une authentification est nécessaire pour accéder à la ressource
<b>404 Not Found</b>	Page non trouvée
<b>500 Internal Server Error</b>	Erreur interne du serveur
<b>503 Service Unavailable</b>	Service temporairement indisponible ou en maintenance

## VII.5.2/ Proxy HTTP (serveur mandataire)

### Qu'est ce qu'un serveur proxy HTTP ?

Un serveur proxy HTTP est une interface entre le client HTTP et le serveur HTTP.

Le client demande les données au serveur proxy qui, suivant le cas, les demande à son tour au serveur HTTP cible.



- 1/ Requête HTTP du client
- 2/ La page demandée est elle en cache ? Si oui => 6
- 3/ Requête HTTP au serveur cible
- 4/ Réponse du serveur (code + page)
- 5/ Mise en cache de la page
- 6/ Réponse au client (code + page)

# Les avantages

## **Optimisation de la bande passante**

Le serveur proxy garde en mémoire (cache) un certain temps les données téléchargées. Si vous demandez une page (statique) qui a déjà été téléchargée par le proxy celui-ci vous la renverra immédiatement sans aller la redemander à la source.

Cela peut parfois poser un problème car le document n'est plus à jour !

## **Authentification, surveillance et filtrage de l'accès à l'Internet**

Le serveur proxy centralise toutes les requêtes HTTP. Par conséquent il est possible de demander une authentification à l'utilisateur.

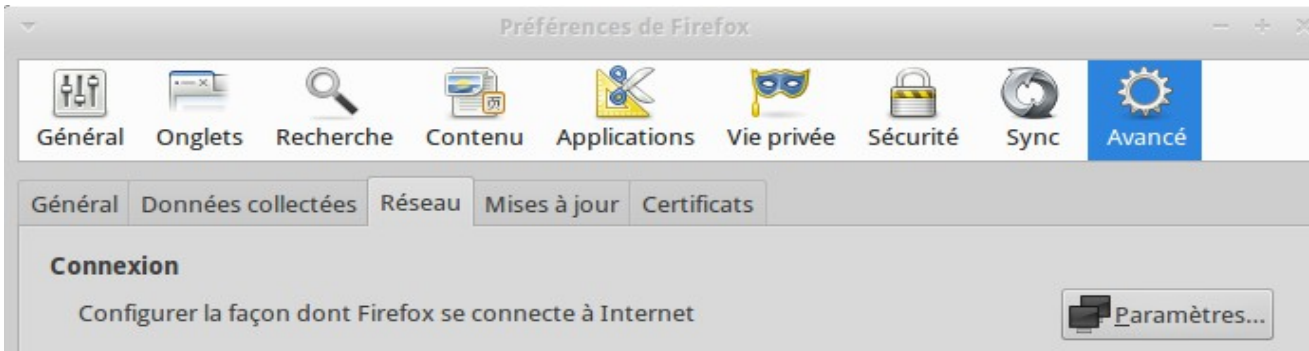
De ce fait toutes ses navigations seront « enregistrées » et conservées sur le serveur proxy.

De même il sera possible de fermer l'accès à certains sites voire à certains contenus.

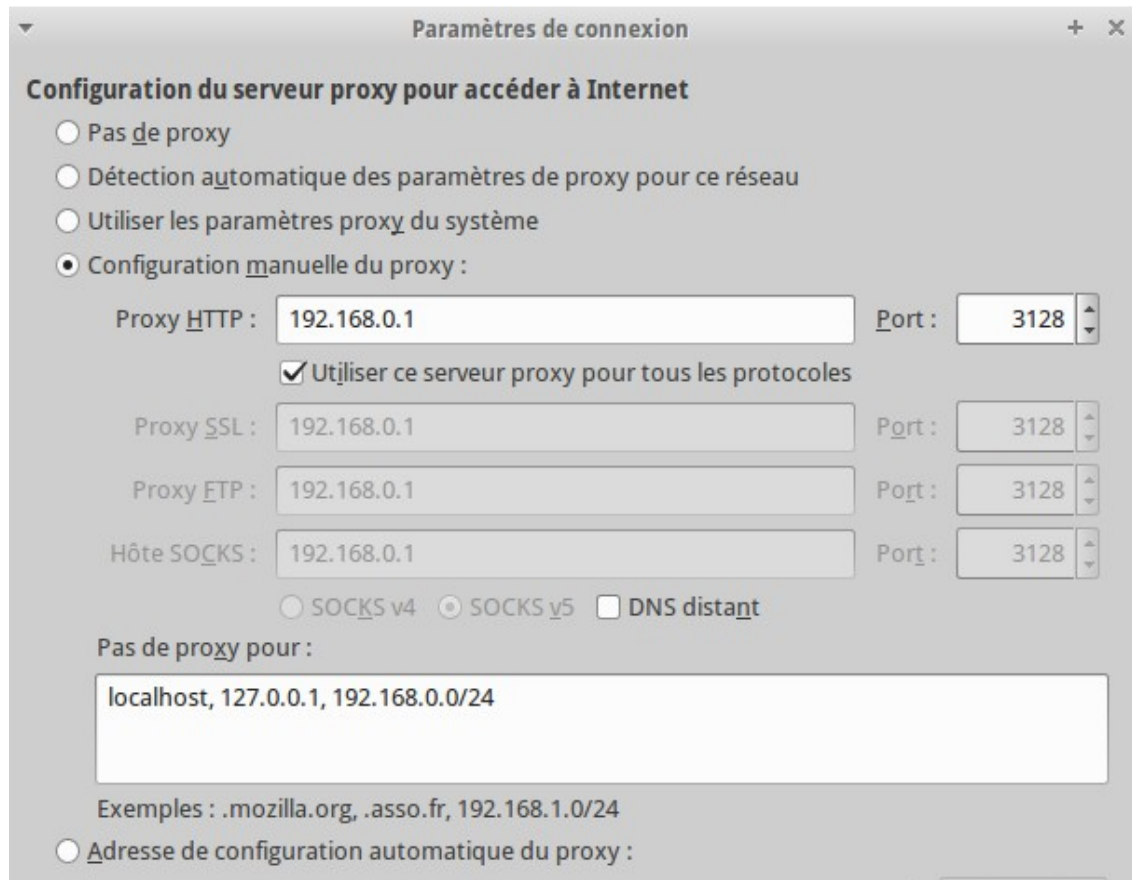




# Configuration du navigateur firefox dans l'atelier GE



L'utilisation d'un proxy HTTP doit être transparente pour l'utilisateur, par conséquent il est nécessaire de configurer Correctement son navigateur.



# Test de la connectivité avec la passerelle/proxy

S'assurer au préalable que votre machine possède une adresse IP valide :

Commande *ifconfig* (ou *ipconfig* sous windows)

Vous devez avoir une adresse de la forme 192.168.0.XX avec XX compris entre 20 et 80

La passerelle/proxy dans l'atelier GE ne réponds pas aux requêtes ICMP (donc au ping) par conséquent on ne peut pas faire un test de connectivité avec la commande *ping* (impossible de *pinguer*)

En revanche, on peut se connecter sur le port 3128 (port du proxy)

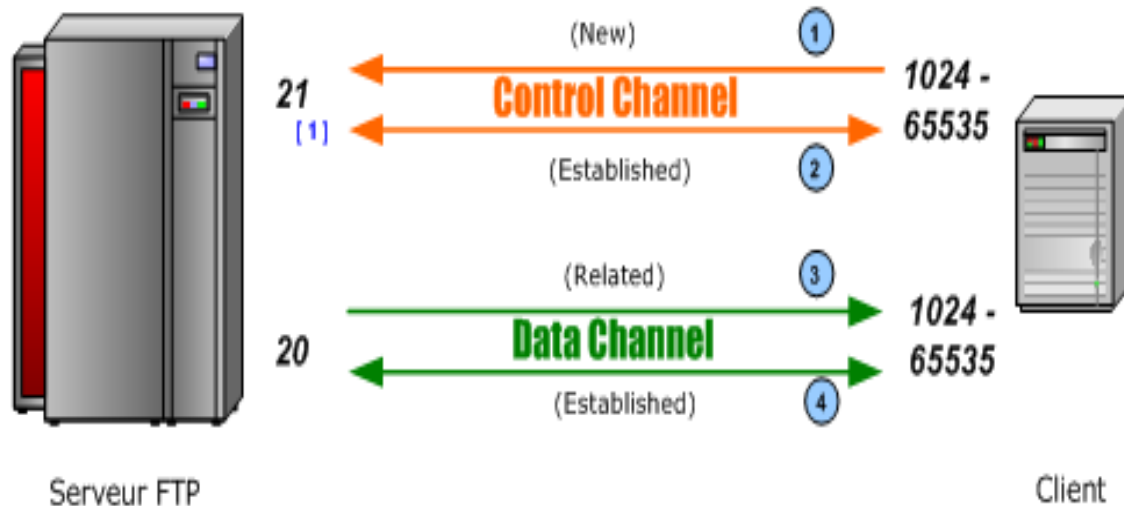
Commande : *telnet 192.168.0.1 3128*

Si la connexion s'établit c'est que la connectivité est assurée.

Dans le cas contraire, pas de connexion possible avec la passerelle ou serveur proxy planté!

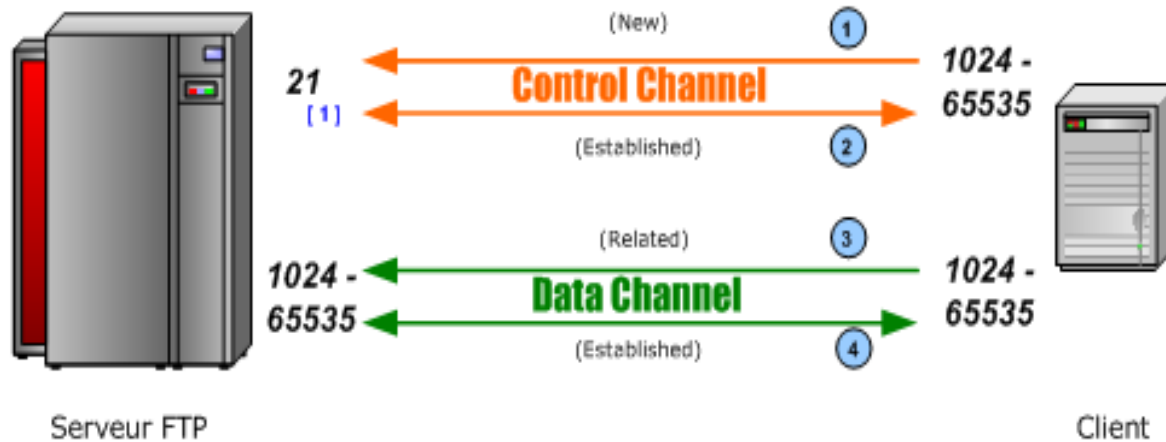
## VII.6/ FTP

### Diagramme FTP actif



**Mode actif:** c'est le client FTP qui détermine le port de connexion à utiliser pour permettre le transfert des données

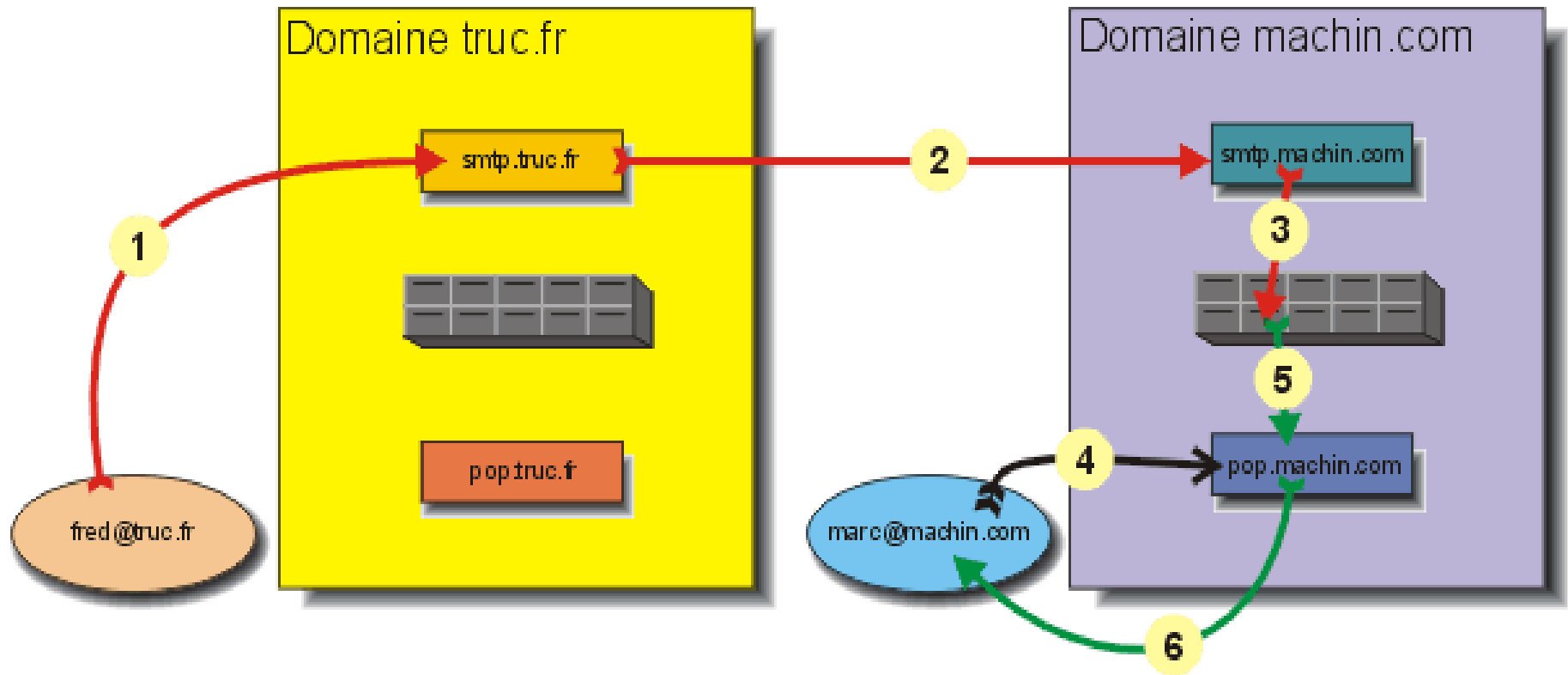
## Diagramme FTP passif



**Mode passif:** le serveur FTP détermine lui même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client.

## VII.7/ Courrier électronique

Transport et réception de courrier.

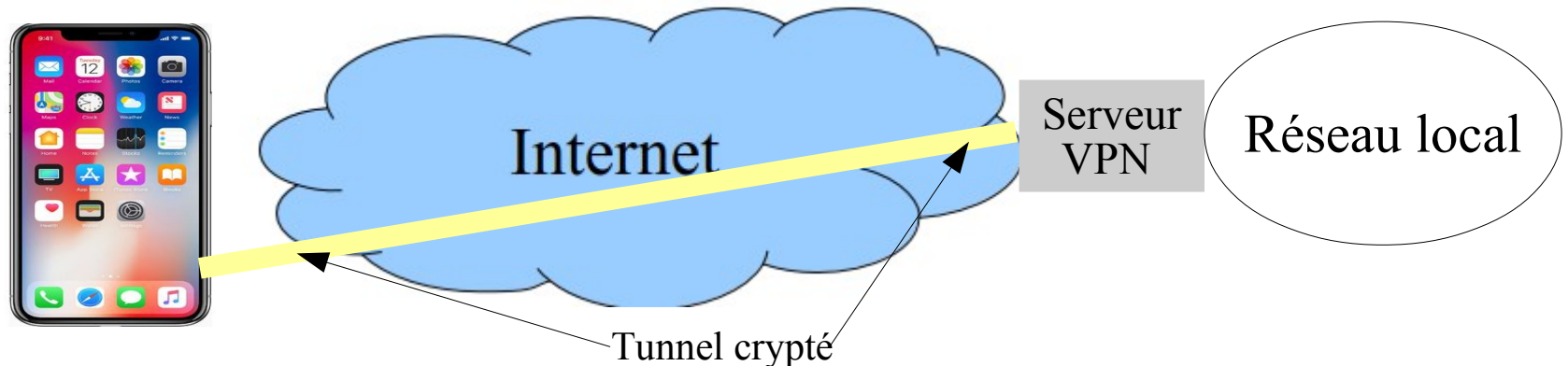


## VII.8/ Les Virtual Private Network (VPN)

Un VPN permet de créer une liaison virtuelle (tunnel de communication entre un client VPN et un serveur VPN) entre deux réseaux physiques distants de manière transparente. Les données étant chiffrées la liaison virtuelle, bien qu'utilisant un réseau public, la plus part du temps Internet, est sécurisée.

Le serveur VPN (la sortie du tunnel) peut amener sur :

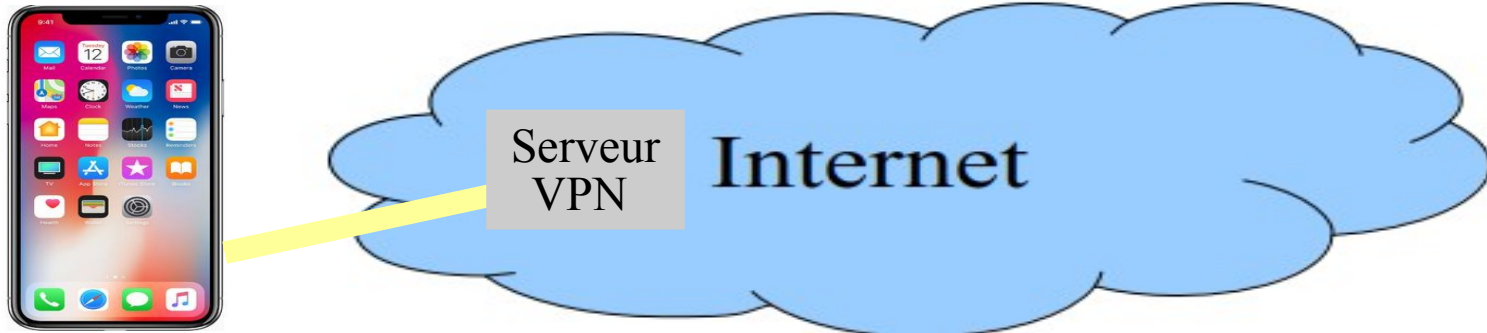
**\*Un réseau local, dans ce cas on est considéré comme appartenant à ce réseau :**



### Exemples :

Télétravail, on utilise les ressources du réseau de l'entreprise à partir de n'importe où  
Le serveur VPN peut être notre BOX, on utilise ses ressources privées (données, applications, services) de la même manière que si on était chez soi.

**\*Amener sur Internet et donc naviguer sur le WEB à travers lui :**



**Avantages :**

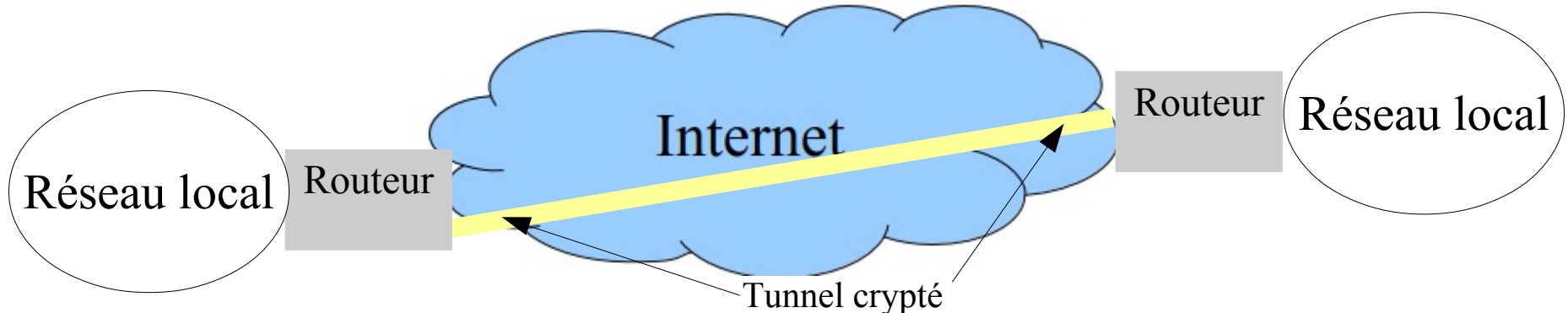
Changer de localisation, navigation comme si on était physiquement dans un autre pays

Dissimulation de votre IP...

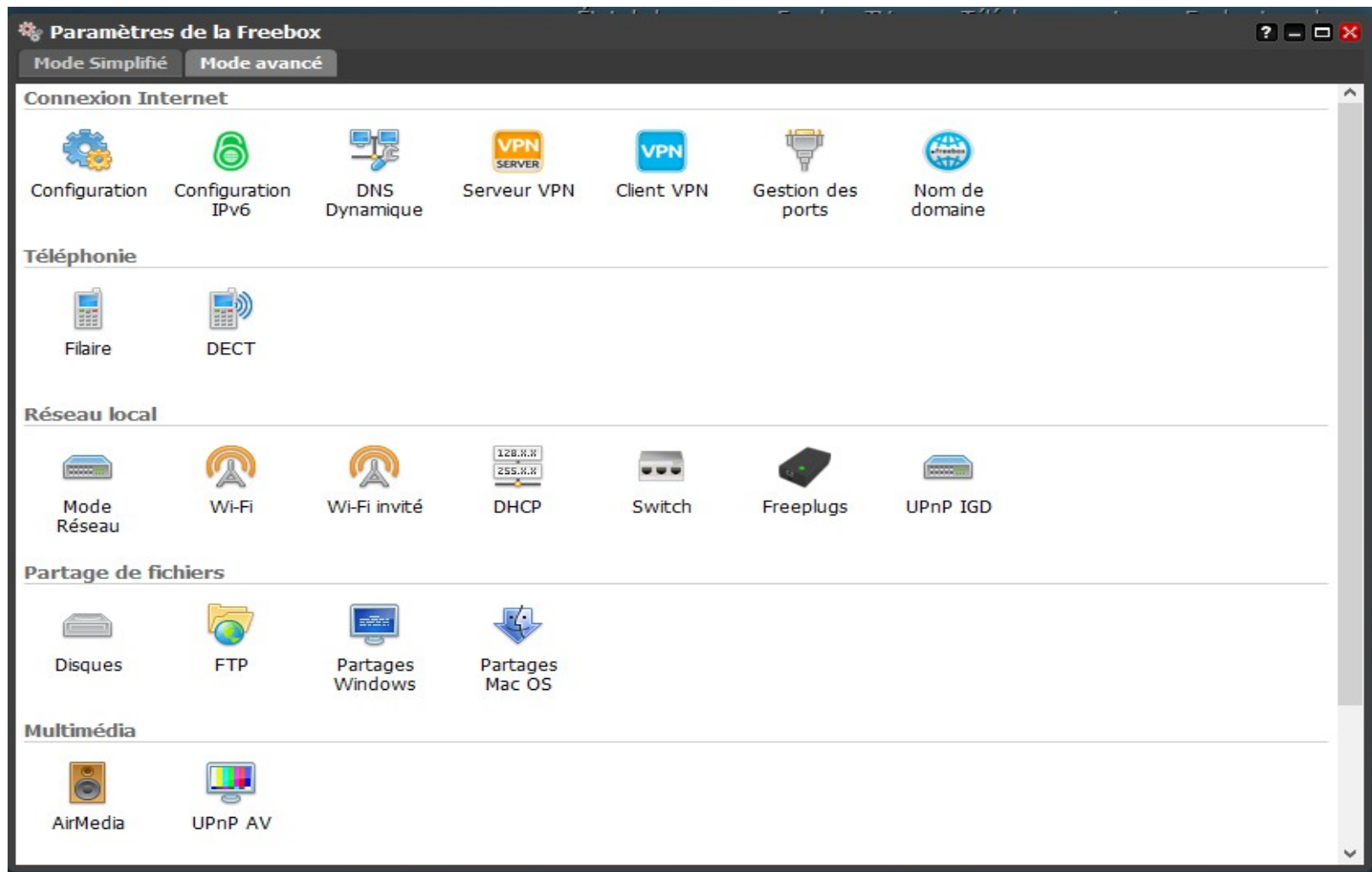
Attention cependant, le serveur VPN n'est pas forcément de confiance...

**\*Relier deux routeurs**

Il s'agit dans ce cas d'une extension de réseau (interconnexion à travers Internet)



# VIII/ Configuration d'une BOX





# Serveur VPN (PPTP)

The screenshot shows a web-based configuration interface for a VPN server. The title bar reads 'Serveur VPN'. On the left is a sidebar with a tree view containing 'État', 'Connexions', 'Configuration', 'Utilisateurs', 'IPsec IKEv2', 'PPTP' (highlighted), 'OpenVPN Routé', and 'OpenVPN Bridgé'. The main content area is titled 'Configuration PPTP' and contains the following settings:

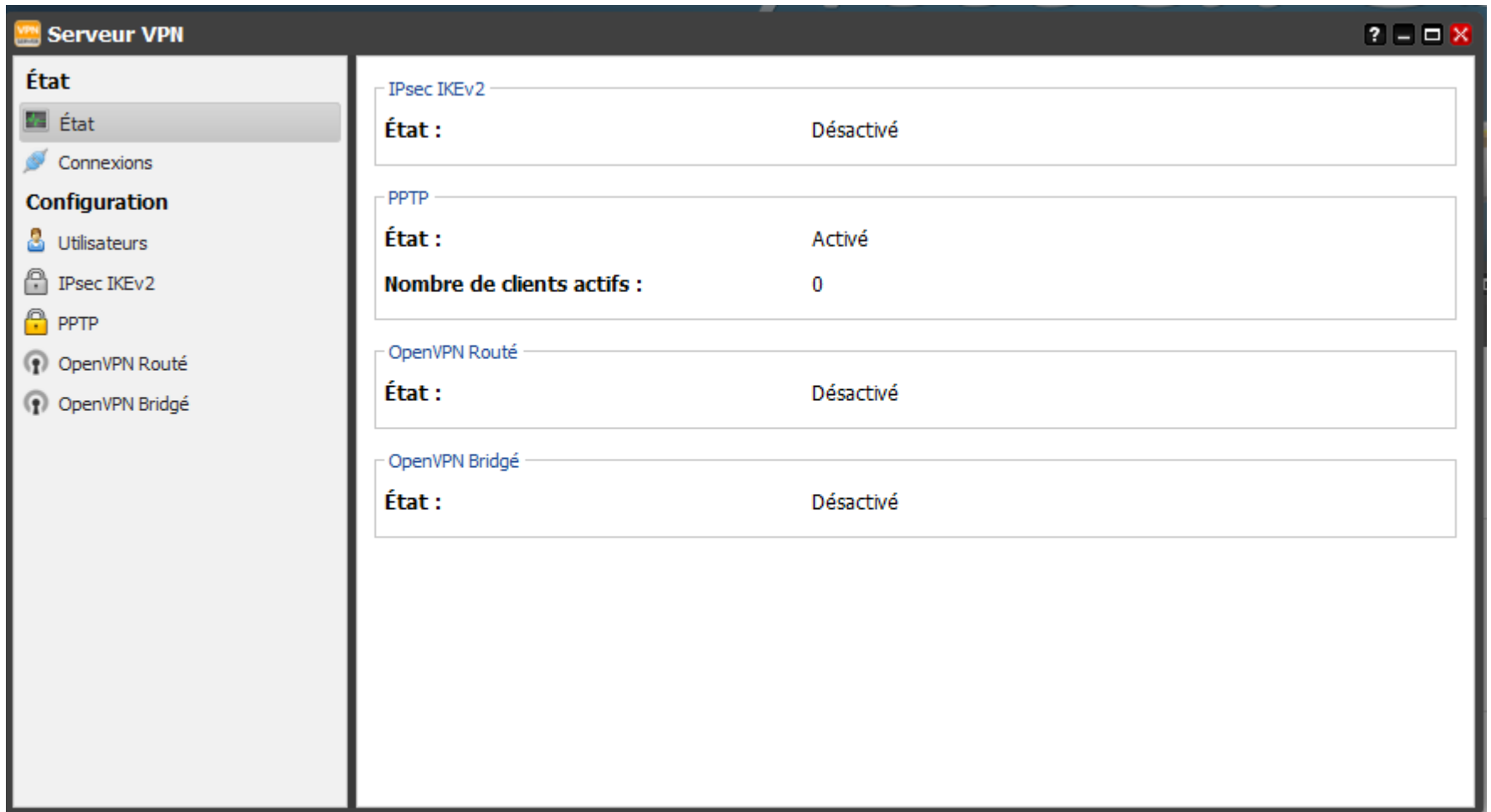
- Activer :** ☒
- Port :** 1723
- Mode de chiffrement :** Obligatoire 128 bits

Below these is a section titled 'Modes de chiffrement autorisés' with three options:

- PAP :** ☐
- CHAP :** ☐
- MS-CHAPv2 :** ☒

At the bottom right are three buttons: a green checkmark icon with 'OK', a red 'X' icon with 'Annuler', and a blue floppy disk icon with 'Appliquer'.

# Config Serveur VPN



**Serveur VPN**

**État**

- État
- Connexions

**Configuration**

- Utilisateurs
- IPsec IKEv2
- PPTP
- OpenVPN Routé
- OpenVPN Bridgé

**IPsec IKEv2**

État : Désactivé

**PPTP**

État : Activé

Nombre de clients actifs : 0

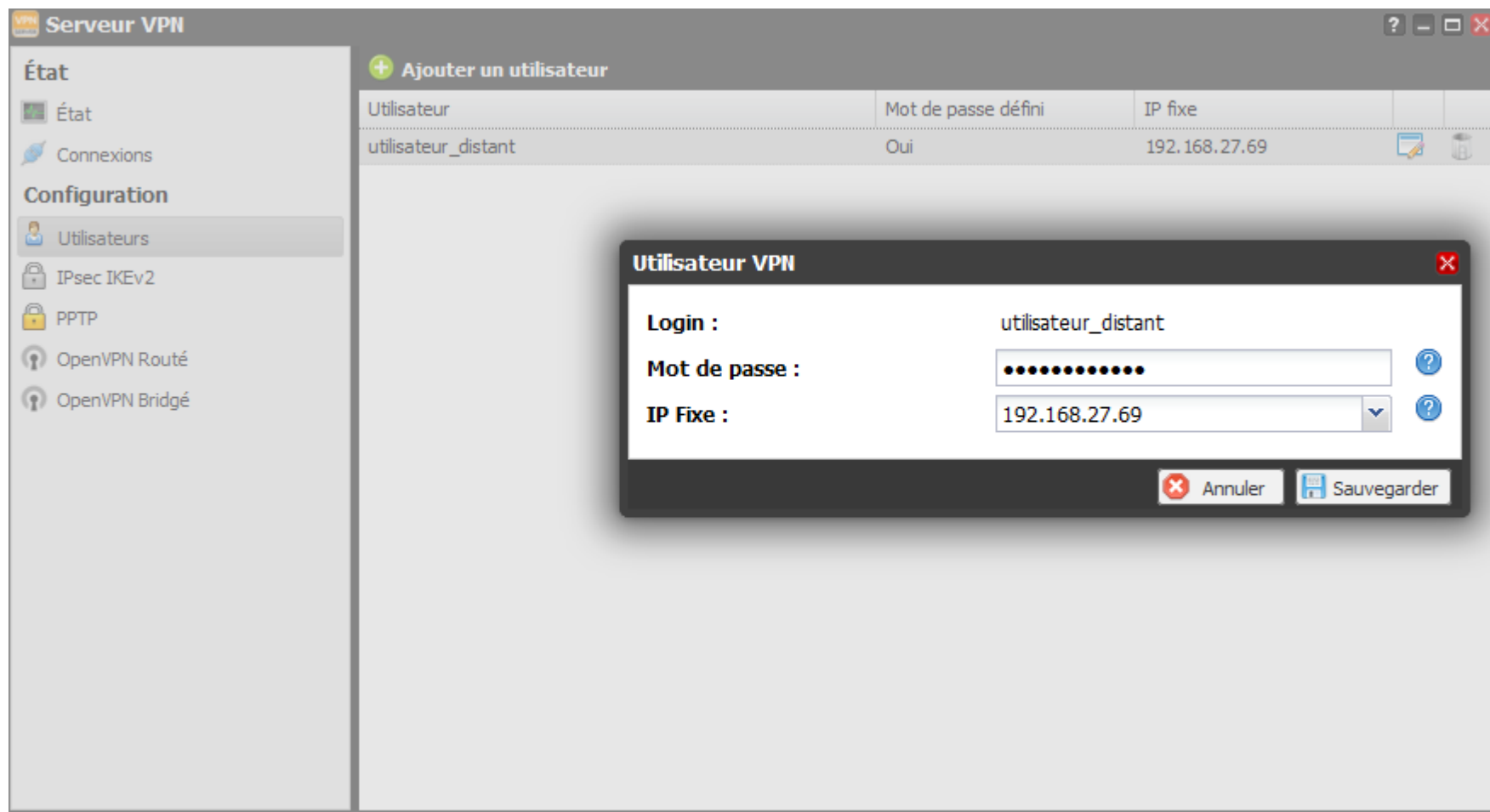
**OpenVPN Routé**

État : Désactivé

**OpenVPN Bridgé**

État : Désactivé

# Serveur VPN (Ajout d'un utilisateur)



# Configuration d'un client VPN sous Windows7

## Configurer un VPN en PPTP ou en L2TP / IPsec

Passons maintenant aux choses sérieuses. Pour configurer un VPN sur Windows en PPTP ou en L2TP / IPsec, ce n'est pas très compliqué. **Notez cependant que toutes les instructions qui suivent valent pour Windows 7 et uniquement pour ce dernier.** Si vous avez une machine tournant sous Windows XP, il faudra donc adapter ce tutoriel. Même chose d'ailleurs pour Windows 8 qui est attendu pour cette année et qui devrait sans doute proposer des options différentes.

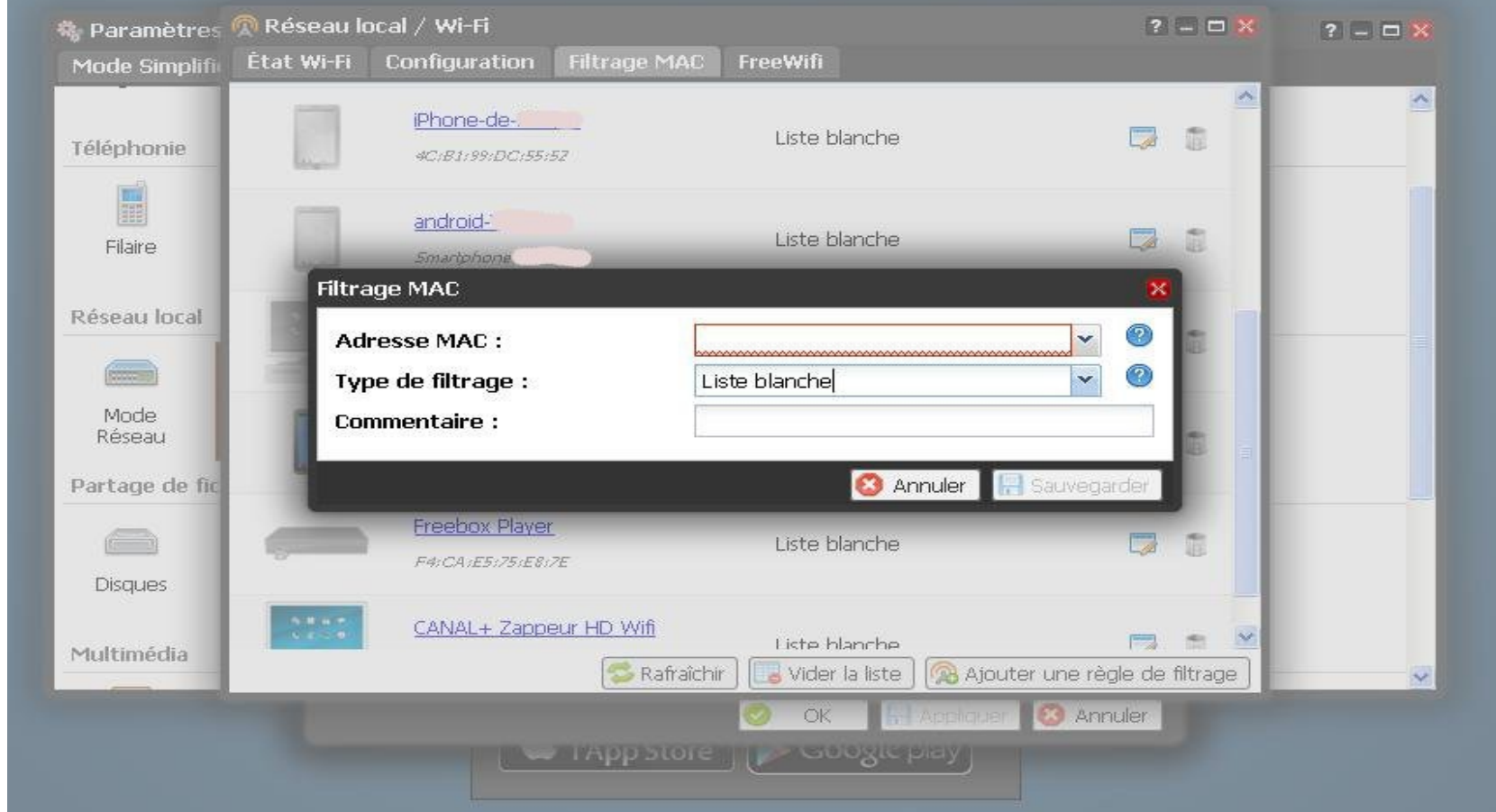
Bref, pour configurer un VPN en **PPTP / L2TP / IPsec** sur Windows, suivez simplement les étapes suivantes :

- Cliquez sur l'icône réseau dans la zone de notification.
- Cliquez sur « Ouvrir le centre réseau et partage ».
- Cliquez sur « Configurer une nouvelle connexion ou un nouveau réseau ».
- Sélectionnez « Connexion à votre espace de travail ».
- Cliquez sur le bouton « Suivant ».
- Sélectionnez « Utiliser ma connexion Internet (VPN) ».
- Saisissez l'adresse de votre serveur dans le champ « Adresse Internet ». (\*)
- Donnez un nom à votre connexion.
- Cliquez sur le bouton « Suivant ».
- Saisissez votre nom d'utilisateur dans le premier champ. (\*)
- Saisissez votre mot de passe dans le second champ. (\*)
- Cochez la case « Mémoriser ce mot de passe ».
- Cliquez sur « Connecter ».

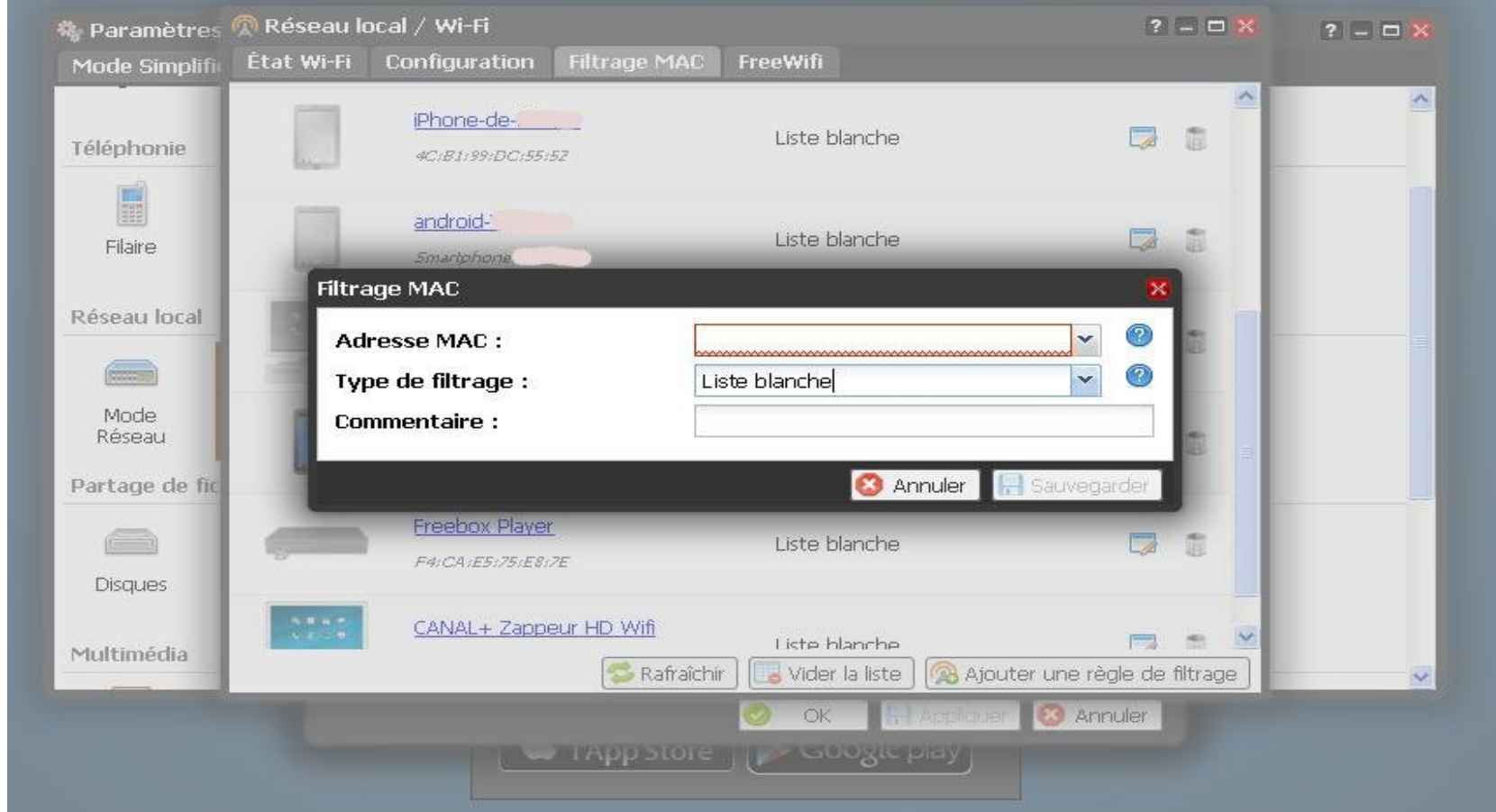
# WI-FI



# WI-FI : restriction d'accès sur la base d'@ MAC



# WI-FI : restriction d'accès sur la base d'@ MAC



# Redirection de port





# DHCP réseau privé

