http://WWW.CABARE.NET ©

Technique de Base Câblage LAN et WIFI

Gestion réseaux Ethernet 802.x

Michel Cabaré – Ver 1.6 – déc 2017-

Technique de Base Câblage Lan & WIFI

Gestion Réseaux Ethernet 802.x

Michel Cabaré – Ver 1.6 – Déc 2017

www.cabare.net ©

Table des matières

LA NORME ETHERNET

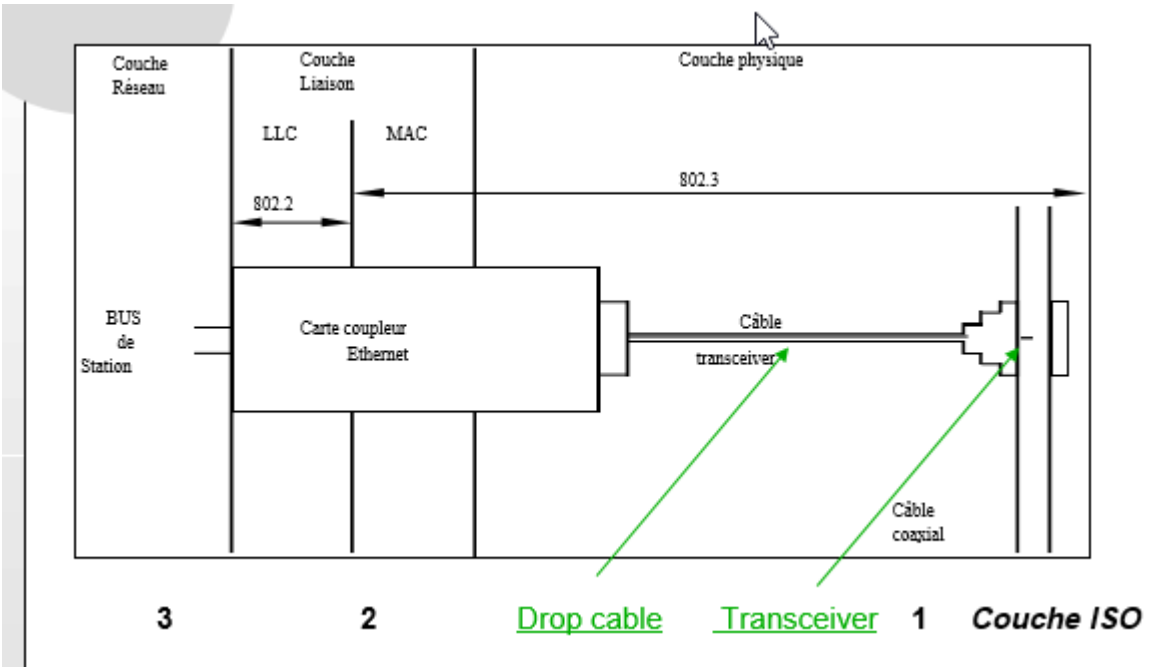
Présentation générale :

La Norme Ethernet à été développée par XEROX dans les années 1970 et fit l'objet de spécifications normalisée sous la poussée d'un consortium de 3 entreprises dans les années 1980 DEC - INTEL - XEROX .

En 1985, l' IEEE (Institute of Electrical and Electronic Engineers) publia la norme définitive sous l'apellation IEEE 802.3 CSMS/CD.

Depuis la norme à constamment évolué pour tenir compte des nouveau type de media disponibles et débit possibles.

Elle occupe la couche 1 et 2 dans le Modèle ISO



A ce titre on distingue principalement quatres catégories, selon le débit nominal du média, à 10Mbps - 100Mbps - 1000Mbps…et les réseaux sans fils

Trame Ethernet 802.3 :

La Norme Ethernet à été développée par XEROX dans les années 1970 et fit l'objet de spécifications normalisée sous la poussée d'un consortium de 3 entreprises dans les années 1980 DEC - INTEL - XEROX .

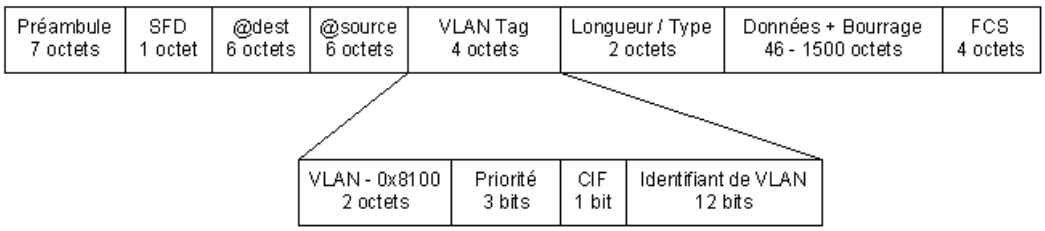
Préambule 7 octets	SFD 1 octet	@dest 6 octets	@source 6 octets	EtherType 2 octets	Données 46 - 1500 octets	FCS 4 octets

- Le **préambule** est une séquence de 56 bits alternant les valeurs 0 et 1 utilisées pour la synchronisation. Cela permet à toutes les stations de détecter la présence du signal et de se préparer à la réception de la trame. Le délimiteur de trame (**SFD** : Start Frame Délimiter) est la séquence 10101011 qui indique le début de la trame.
- Les **adresses MAC source et destination** identifient de façon unique les stations qui émettent et reçoivent les données. Le standard permettait à l'origine d'utiliser des adresses sur 2 ou 6 octets, mais seule la version 6 octets est utilisée en pratique. L'adresse destination peut être une adresse unicast (une seule station), une adresse multicast (un groupe de station), ou une adresse de broadcast (FF-FF-FF-FF-FF-FF) qui indique l'ensemble des stations du réseau.
- Le champ **Longueur / Type** donne soit l'identifiant du protocole de niveau supérieur OSI (Ethernet) s'il est supérieur à 1536 (par exemple, 2048 pour IP), soit le nombre d'octets du champ Données (trame 802.3) s'il est inférieur à 1500.
- **Ether Type** spécifie le protocole à utiliser : Par exemple, si c'est IPv4, ce champ vaudra 0x0800 (la valeur 0800 en hexadécimal). Si c'est ARP, il vaudra 0x0806… etc
- Le champ **Données** comprend au maximum 1500 octets. S'il est inférieur à 46 octets, le champ Bourrage devra être rempli en conséquence : au total, les champs Données et Bourrage doivent être compris entre 46 et 1500 octets.
- Le champ **FCS** (Frame Check Sequence) contient un CRC (Cyclical Redundancy Check) sur 4 octets utilisé pour le contrôle d'erreur. Ce CRC est calculé sur les données comprises du champ d'adresse Destination jusqu'au champ de Bourrage.

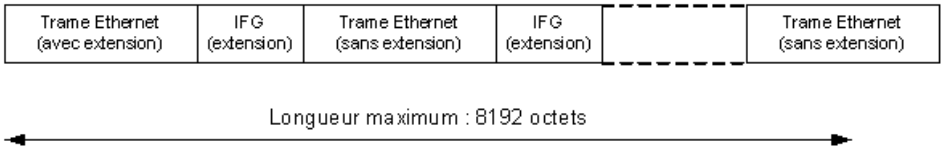
La trame Ethernet doit avoir une longueur minimum de 64 octets et maximum de 1518 octets depuis l'adresse MAC Destination au champ FCS. Le préambule et le SFD ne sont pas inclus.

Evolutions

1. La norme **802.3ac** (1998) a étendu la longueur maximum de la trame à 1522 octets pour permettre l'ajout d'une étiquette VLAN (Virtual Local Area Network Tagging) sur 4 octets



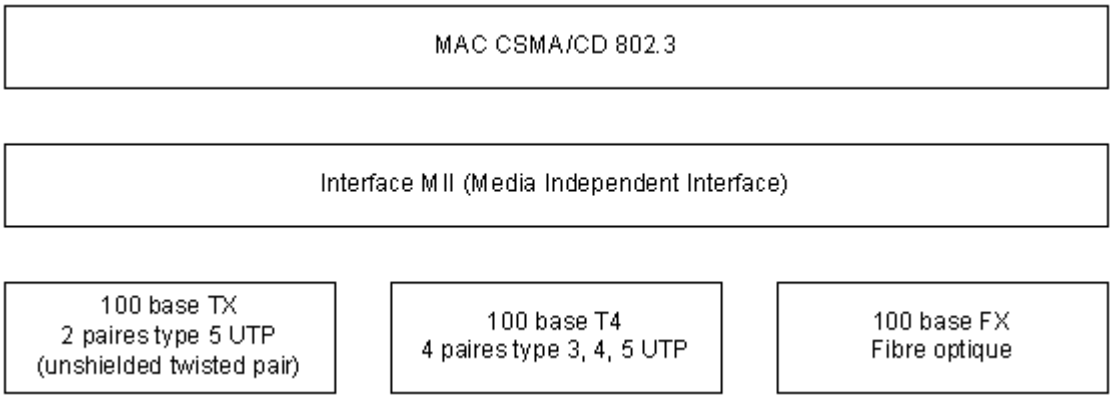
2. Avec l'introduction du standard **802.3z** en 1998 (Gigabit Ethernet), un champ d'extension a été ajouté à la fin de la trame Ethernet



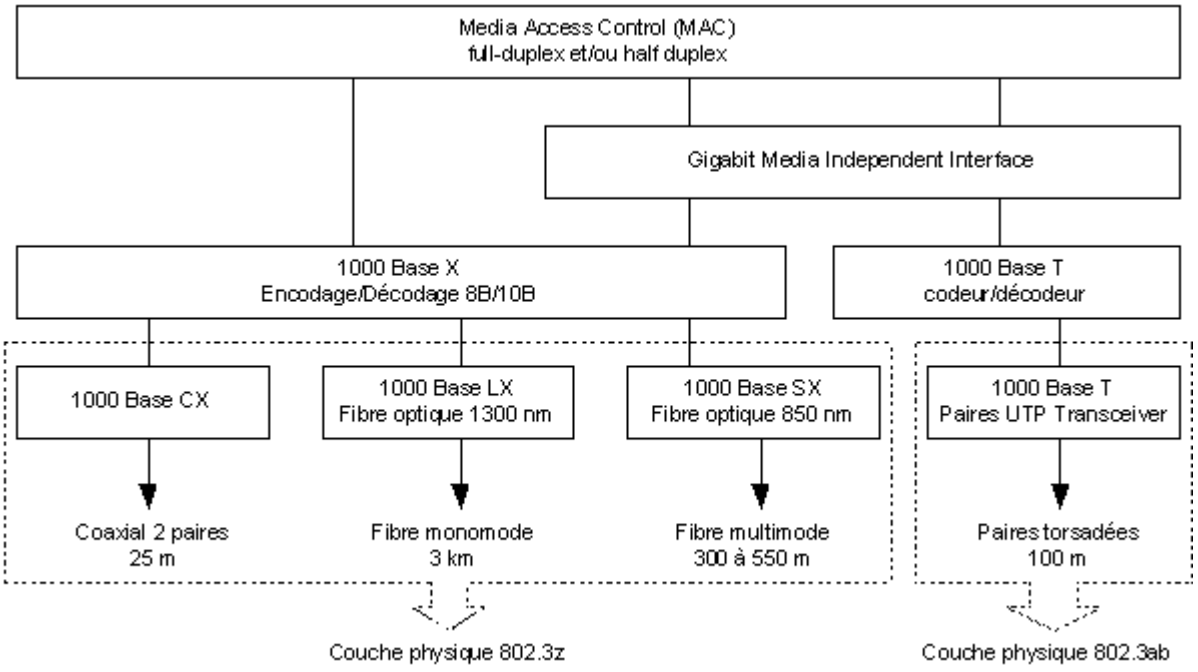
N.B : Cette extension n'est nécessaire qu'en mode half-duplex, puisque le protocole de détection de collision n'est pas utilisé en full-duplex.

Le Gigabit Ethernet introduit également un nouveau mode de transmission : le burst mode, ou mode rafale. Ce mode rafale est optionnel, et permet à une station de transmettre une série de trame sans interruption sur le média. Utilisé en half-duplex uniquement, cette fonction permet d'optimiser la performance des réseaux Gigabit Ethernet en cas de transmission d'une série de trames courtes.

L'Evolution 100 Base-T



Désormais, de nos jours on rencontre plutôt les évolutions 1000 Base : (Et 10G)



à **10 Mbps** (ETHERNET) on distinguera :

10 BASE 5 :	**Thick Coax** (Coaxial épais)	**802.3**
10 BASE 2 :	**Thin Coax** (Coaxial fin)	**802.3a**
10 BASE T :	**Twisted Pair** (Paires torsadées)	**802.3i**
10 BASE F :	**Fiber Optic** (Fibre Optique)	

à **100 Mbps** (FAST ETHERNET) on distinguera :

100 BASE TX :	**Twisted Pair** (Paires torsadées)	**802.3u**
100 BASE T4 :	**4 Twisted Pair** (4 Paires torsadées)	**802.3**
100 BASE FX :	**Fiber** (Fibre optique)	**802.3**

à **1000 Mbps** (GIGABIT ETHERNET) on distinguera :

1000 BASE CX :	**Coax** (Coaxial épais)	**802.3z**
1000 BASE LX :	**Fiber** (Fibre optique 1300nm)	**802.3z**
1000 BASE SX :	**Fiber** (Fibre optique 850nm)	**802.3z**
1000 BASE T :	**Twisted Pair** (4 Paires torsadées)	**802.3ab**

à **10000 Mbps** (10 GIGABIT ETHERNET ou 10Gbe) on distinguera uniquement et principalement pour notre usage en LAN

10G BASE SR :	**Fiber** (multi-mode 850nm)	**802.3ae**
10G BASE LR :	**Fiber** (mono-mode 1300nm)	**802.3ae**
10G BASE ER :	**Fiber** (mono-mode 1550nm)	**802.3ae**
10G BASE LRM :	**Fiber** (multi-mode 1310nm)	**802.3ae**
10G BASE T :	**Twisted Pair** (4 Paires torsadées)	**802.3an**

N.B: La dernière norme apparue en Septembre 2016 définit les 2.5 Gigabit and 5 Gigabit Ethernet over Cat-5/Cat-6 twisted pair

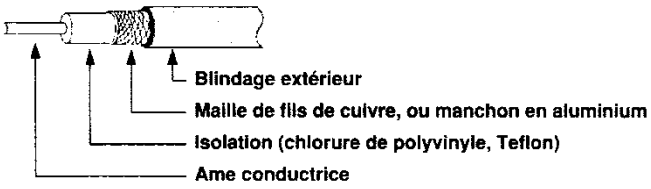
[802.3_NGBASET] FW: Approval of IEEE Std 802.3bz 2.5GBASE-T and 5GBASE-T

2.5G BASE T :	**Twisted Pair** (4 Paires torsadées)	**802.3ng**
5G BASE T :	**Twisted Pair** (4 Paires torsadées)	**802.3ng**

d'autres évolutions **sans fils** existent

LAN - CABLAGE ETHERNET

Coaxial :

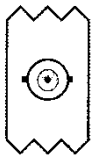


Les câbles coaxiaux les plus courant sont

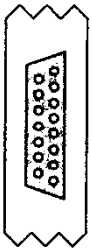
- **RG11** ou **Ethernet épais** ou **Thicknet** : Il servait généralement d'épine dorsale d'un réseau en Ethernet et réponds au standard 802.3 10Base5. Obsolète

  N.B: Le câble large bande des réseaux de télévision NE REPONDS PAS AUX NORMES RESEAUX (notamment par son impédance de 75 ohms)

Les prises associées étaient :



BNC pour le Thinnet



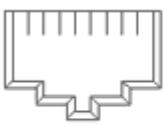
AUI pour le Thicknet

Un **té de raccordement** placé sur la carte réseau de chaque station ou du serveur sert de point d'arrivée et de départ du **câble coaxial** pour d'autres stations. Chaque station située en fin de réseau est munie d'un **bouchon terminal** nécessaire à une bonne transmission des signaux informatiques

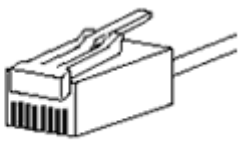
Twisted Pair - Paires torsadées :

Les paires sont assemblées en câbles multi-paires comportant 2-4-6-8-14-25-56-112-224 paires. Ils sont conçu ainsi afin de minimiser les interférences avec l'extérieur et les effets de diaphonie.

Les prises associées sont dites **RJ45** pour UTP ou STP (identique visuellement à la RJ11 Téléphonique)



RJ45 Femelle



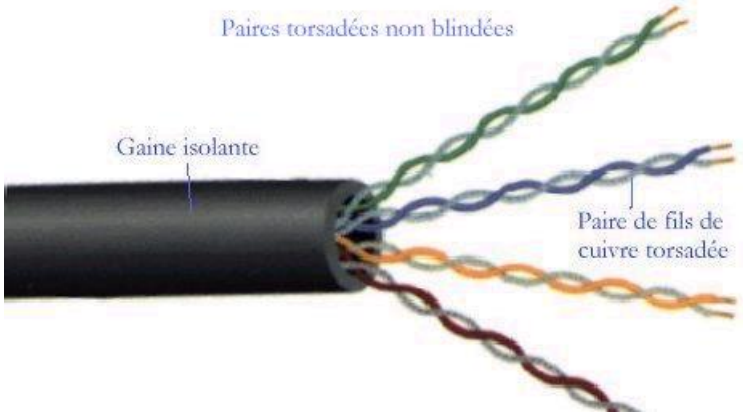
RJ45 Mâle

Principe du blindage :

Les câbles à paires torsadées les plus courants sont

- **Paires Torsadées Non Blindées** ou **UTP** ou Unshielded Twisted pairs.

Que l'on peut avoir de différentes qualité selon leur bande passante



Léger, facile à poser, économique ils n'autorisent pas cependant de très haut débits mais peuvent atteindre 100 Mégabit/s. Sur de longues distances 1Km, ils chuteront sur un débit de 1Megabits/s

- **Paires Torsadées Blindées** ou **STP** ou Shielded Twisted pairs.

Que l'on peut avoir de différentes qualités selon leur bande passante. Le blindage nécessitant une mise à la masse parfaite!

F Foiled Ecrantage (feuillard aluminium) - S shield blindage (tresse cuivre):

On peut distinguer un blindage par feuille d'aluminium, ou un blidange par tresse de fil de cuivre

F = Foiled = écrantage / S = Shield = blindage / U = Unshielded = Rien

On aura donc

- **TP** = twisted pair paire torsadée
- **U** = unshielded non blindé
- **F** = foil shielding blindage par feuillard
- **S** = braided shielding blindage par tresse

Et bien sûr, le blindage peut être appliqué individuellement aux paires, ou à l'ensemble formé par celles-ci. Donc il peut être "externe" au cable ou "interne" autour de chaque paire torsadée.

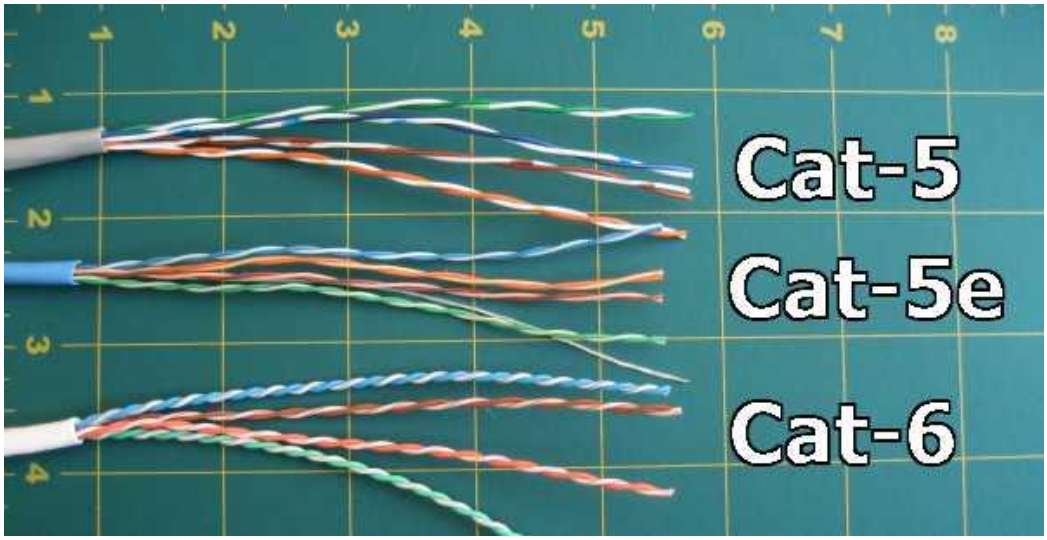
Câbles UTP - STP - FTP - FFTP - SFTP - SSTP

- UTP (Unshielded Twisted Pair) est un câble RJ45 non blindé, non écranté.
  U/UTP
- STP (Shielded Twisted Pair) est un câble RJ45 écranté paire par paire. Chaque paire torsadée est donc blindée individuellement
  U/UTP
- FTP (Foiled Twisted Pair) est un câble RJ45 écranté avec une feuille d'aluminium. L'ensemble des paires torsadées a un blindage global disposé entre la gaine extérieure et les 4 paires torsadées. Les paires torsadées ne sont donc pas individuellement blindées
  F/UTP
- FFTP (Foiled foiled twisted pair) -. Chaque paire torsadée est entourée d'une feuille de blindage en aluminium. L'ensemble des paires torsadées a une feuille de blindage collectif en aluminium.
  F/FTP
- SFTP (Shielded Foiled Twisted Pair) est un câble RJ45 écranté paire par paire et blindé. Câble donc doté d'un double écran (feuille métallisée et tresse) commun à l'ensemble des paires. Les paires torsadées ne sont donc pas individuellement blindées (contrairement à ce que le terme Shielded foiled twisted pair pourrait laisser faire croire).
  SF/UTP
- SSTP (Shielded and Shielded Twisted Pair) est un câble RJ45 blindé paire par paire avec un blindage autour. Chacune des paires est blindée par un écran en aluminium, et en plus la gaine extérieure est blindée par une tresse en cuivre étamé
  S/FTP

Dénomination courante	Dénomination officielle	Blindage de l'ensemble du câble	Blindage des paires individuelles
UTP	U/UTP	aucun	aucun
STP	U/FTP	aucun	feuillard
FTP	F/UTP	feuillard	aucun
FFTP	F/FTP	feuillard	feuillard
SFTP	SF/UTP	feuillard, tresse	aucun
SSTP	S/FTP	tresse	feuillard

N.B: en dénomination officielle, Le code avant le slash (la barre oblique) désigne le blindage pour le câble lui-même (l'ensemble des paires torsadées), alors que le code après le slash détermine le blindage des paires individuelles

Selon la catégorie du Câble, la finesse de "torsade" change….



Catégories de câble 3 - 7:

La différente qualité de câble paire torsadée sont données par des caractéristiques fort complexes (diaphonie, bande passante maximale, aténuation selon la longueur…) Quelques caractéristiques principales:

"Catégorie 3" :

conçus pour du transport de voix/données et pour des applications type ethernet 10 Mb/s sur 100 mètres : A ne plus utiliser aujourd'hui

"Catégorie 4" :

applications type token-ring 16 Mb/s

"Catégorie 5" :

applications type ethernet 100 Mb/s sur 100 mètres

"Catégorie 5E améliorée" :

applications type ethernet 2,5 Gb/s sur 100 mètres (10 Gb/s sur 30-50 mètres)

"Catégorie 6 " :

applications type ethernet 5 Gb/s sur 100 mètres (10 Gb/s sur 55 mètres)

"Catégorie 6A améliorée" :

applications type ethernet 10 Gb/s sur 100 mètres

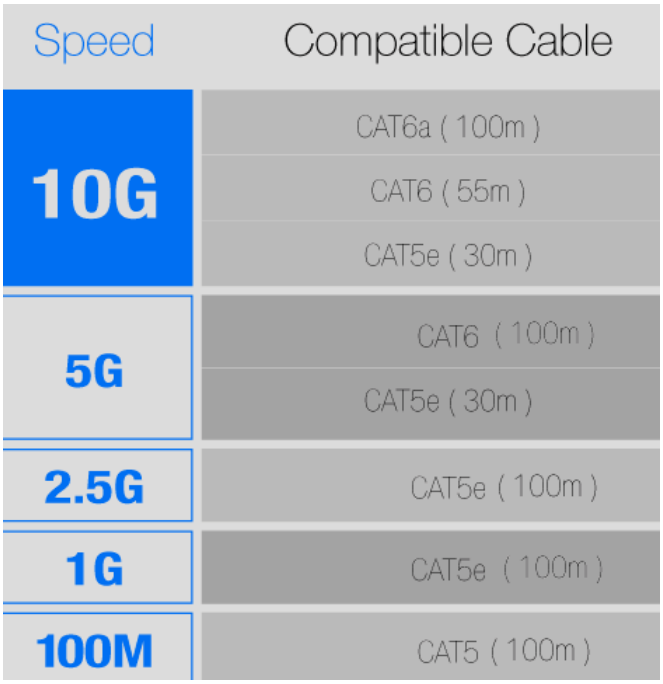
"Catégorie 7" :

applications type ethernet 100 gb/s

	Length (meters)	Speed (Mb/s)		Speed (Gb/s)		Power Over Ethernet	Mhz
		10	100	1	10		
Cat-5	100	X	X			X	100
Cat-5e	100	X	X	X		X	100
Cat-6	100 55 for 10 Gb/s	X	X	X	X	X	250
Cat-6a	100	X	X	X	X	X	500

Cela pourrait se résumer aussi par catégories

ou par débit (avec les nouvelles normes 2.5baseT et 5GbaseT:



Courants Fort – Courants faibles :

Ecartement entre les câbles courant fort (réseau électrique, néon) et courant faible (réseau Ethernet)

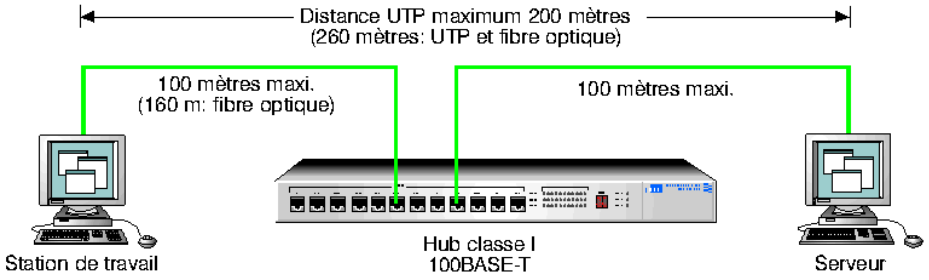
Ecartement en cm									
30 cm									
20 cm									
10 cm									
5 cm									
		10 m		20 m		30 m			80 m
	Cheminement parallèle en mètres								

En 10 -100 Classe de hub :

Il existe deux classes de Hub différentes, selon que les signaux soient simplement répétés ou bien régénérés avant d'être retransmis.

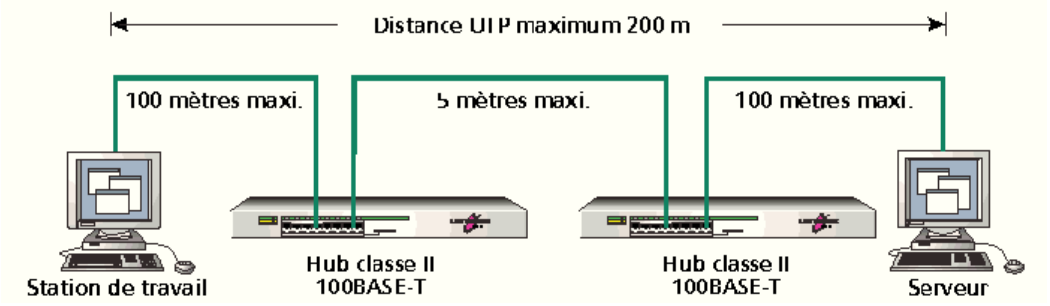
Hub de classe I :

le Hub de "classe I" régénère le signal et le diffuse en l'adaptant au type de port. On peut connecter à un Hub de classe I des typologies 100Base Tx et/ou des typologies 100Base T4 simultanément. En 100 base-T la norme indiquait 1 hub.



Hub de classe II :

le Hub de "classe II " répète immédiatement le signal .On ne peut connecter à un Hub de classe II que des typologies identiques 100Base Tx ou 100Base T4 sans les mélanger ! En 100 base-T la norme est ultra-restrictive : **5 m** !



Mélange UTP et fibre optique:

Type de Connexion	**Mono-type Paire torsadée**	**Mono-type Fibre optique**	**Paire torsadée (T4) + Fibre optique**	**Paire torsadée(TX) + Fibre optique**
Direct Poste à hub	100 m.	412 m.	/	/
1 hub de classe I	200 m. (100 + 100)	272 m. (136 + 136)	231 m. (100t4 + 131fo)	260 m. (100tx + 160fo)
1 hub de classe II	200 m. (100 + 100)	320 m.	/	308 m. (100tx + 208fo)
2 hub de classe II	205 m. (100 + 5 + 100)	228 m. (111fo + 5 + 111fo)	/	216 m. (100tx+ 5 + 111fo) 2200 m. (100tx+2kfo+100tx)

1000BaseT et 10G - norme sur la distance

A partir de l'évolution, Gigabyte et 10G, la norme ne prévoit plus le nombre de hub que l'on peut rencontrer, mais défini uniquement la distance que l'on peut couvrir avec un "brin".

On peut considérer qu'après le passage par 1 seul hubs de classe 2 , le bruit amplifié devient trop important par rapport au message.

Ce n'est pas le cas pour des switchs de classe 1 qui analysent les trames et les réémettent sans se baser sur le signal électrique, mais en émettant la trame comme une machine d'origine. Il n'y a donc plus de limite théorique

Ordre d'autonégociation :

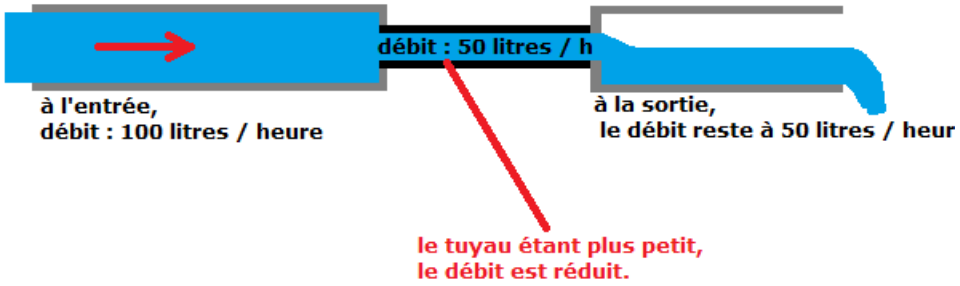
Adaptation de la vitesse de leurs ports (10/100/1000 Mbits/s) à celle de l'appareil qui lui est connecté. dans cet ordre

- 1000BASE-T full duplex
- 1000BASE-T half duplex
- 100BASE-T2 full duplex
- 100BASE-TX full duplex
- 100BASE-T2 half duplex
- 100BASE-T4
- 100BASE-TX half duplex
- 10BASE-T full duplex
- 10BASE-T half duplex

Voire avec les nouvelles Normes 2.5G et 5G selon la nature du câble.

Débit, Latence, Guigue :

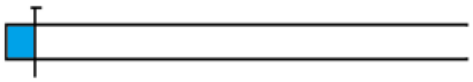
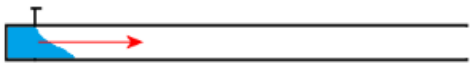
On ne va pas revenir sur le Débit, notion que l'on connait suffisamment bien.



Mais pour évaluer une liaison entre 2 points séparés par plusieurs "hub" / carrefour, on pourrait faire intervenir, outre le nombre de collision, 2 notions nouvelles, la latence, et la Guigue

Latence

La latence correspond au temps entre l'ouverture du robinet et le moment où l'eau arrive à destination. On comprend bien à l'aide de ces schémas que plus le tuyau est long, plus la latence est élevée. (Ce n'est pas une question de débit, car le tuyau pourrait être plus gros, cela ne changerait rien, il faudrait toujours autant de temps à l'eau pour arriver au bout du tuyau).

Etape 1 : le robinet est fermé.	
Etape 2 : j'ouvre le robinet, l'eau entre dans le tuyau	
Etape 3 : l'eau de déplace dans le tuyau	
Etape 4 : l'eau arrive à destination	

Et donc, si nous appliquons ce petit schéma sur un réseau informatique, voici ce que l'on pourrait donner comme définition de la latence :

- La latence est le temps que met un paquet pour arriver d'un ordinateur à un autre ordinateur.
- On comprend bien que plus la latence (le temps) est faible, meilleure est la connexion.

Ainsi le protocole UDP qui peut être utilisé pour transporter des données sur des réseaux IP. fait l'hypothèse que tous les paquets émis sont effectivement reçus par l'autre partie (ou les contrôles de la bonne réception et l'éventuelle ré-émission sont gérés à un autre niveau, par exemple, par l'application elle-même). Donc la vitesse à laquelle les paquets sont envoyés par l'émetteur ne sont pas impactés par le temps nécessaire pour atteindre l'autre partie (ce qui correspond à la latence réseau). Quel que soit ce temps, l'émetteur enverra un certain nombre de paquets par seconde

TCP est un protocole plus complexe qui intègre un mécanisme qui vérifie que chaque paquet est correctement reçu. Ce mécanisme est nommé acquittement : il consiste, pour le destinataire, à envoyer un paquet spécifique ou à indiquer à l'émetteur la bonne réception de chaque paquet.

Pour des raisons d'efficacité, on n'acquittera pas chaque paquet un par un : l'émetteur n'attend pas l'acquittement du paquet précédent pour envoyer les paquets suivants. En fait, le nombre de paquets qui peuvent être envoyés avant de recevoir l'acquittement correspondant est géré par une valeur appelée « fenêtre de congestion TCP (ou reception) » .

Si nous faisons l'hypothèse qu'aucun paquet n'est perdu : l'émetteur enverra un premier quota de paquets (correspondant à la fenêtre de congestion TCP) et quand il recevra le paquet d'acquittement, il augmentera la valeur de la fenêtre de congestion ; progressivement le nombre de paquets qui peuvent être envoyés sur une période données augmentera (débit). Le délai jusqu'à ce que le paquet d'acquittement soit reçu (correspondant à la latence) aura donc un impact sur la rapidité à laquelle la fenêtre de congestion TCP augmentera (et donc sur le rythme auquel le débit s'accroitra).

Quand la latence est élevée, cela signifie que l'émetteur passe plus de temps en attente (sans envoyer de nouveaux paquets) ce qui réduit la vitesse à laquelle le débit s'accroit

- En fibre optique la latence est quasi-nulle,
- elle est un peu plus élevée en connexion par câble RJ45
- c'est en Wifi que la latence est la plus élevée.

Guigue

la gigue exprime la variation de la latence.

Il est tout à fait possible d'avoir une latence élevée, par exemple de 200ms, et d'avoir une gigue très faible. Cela veut dire que la latence est toujours la même.

Le problème d'une gigue élevée (donc une latence qui n'arrête pas de varier), c'est que par moment les paquets vont arriver tous d'un coup, et par moment aucun paquet n'arrivera.

Dans une visioconférence ou une conférence téléphonique, il faut que le débit de parole ou d'image soit le plus fluide possible. Sinon, voici ce qui pourrait se passer

La personne A parle

Ses paroles sont envoyées vers B

La latence devient plus élevée qu'avant

ses paroles n'arrivent plus, Le flux reprend avec le nouveau décalage du à la nouvelle latence.

La latence redevient plus faible

Les paroles qui étaient déjà en cours d'acheminement, et celle que A prononce actuellement arrivent toute en même temps. Le logiciel doit faire un tri, et tout n'est pas audible.

La personne B perd des morceaux des phrases prononcées par A.

etc…

POE – POWER OVER ETHERNET

Objectif alimentation électrique :

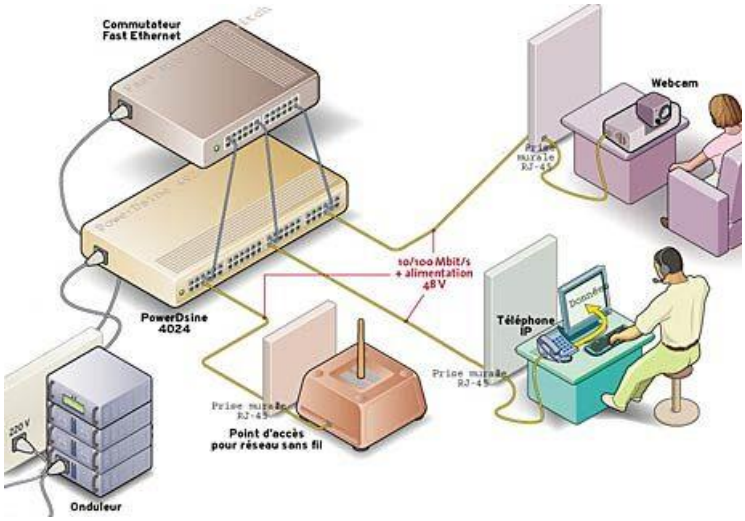
En évolution existe encore sous l'appellation **Power over Ethernet**, normalement référencée sous la norme IEE **802.3af** sortie en juin 2003 !

Les enjeux de cette technologie sont les suivants :

- simplifier l'administration des réseaux Ethernet,
- les faire fonctionner même en cas de coupure d'électricité
- permettre à des équipements de type téléphones IP, point d'accès Bluetooth ou bornes Wi-Fi de fonctionner grâce à une seule alimentation : le câble qui les relie au réseau IP, via la prise RJ 45.

Le courant transite sur 2 paires de fils parmi les 4 d'un cable torsadé, soit sur des paires non employées, soit a des fréquences ne dérangeant pas ces dernières.

Le voltage est de l'ordre de 44 à 57 V pour une puissance maximale de 15Watts, et pour une distance maximale de 100m…

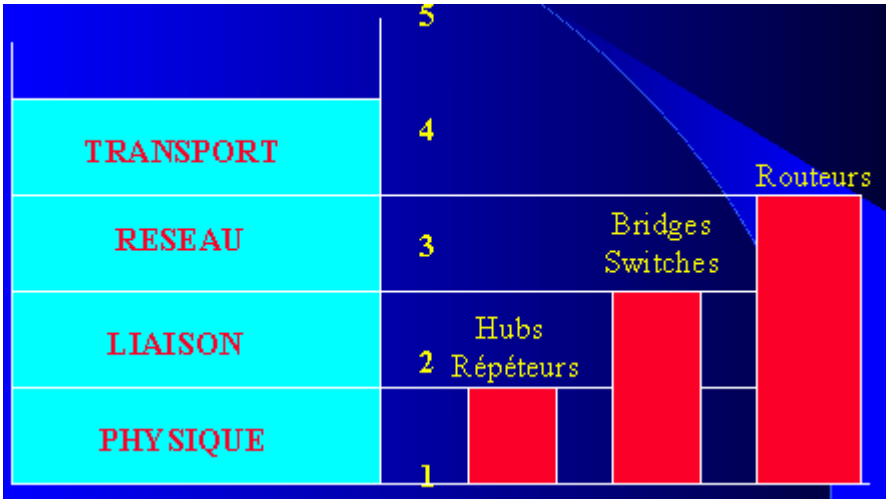


HUB-SWITCH-ROUTEUR…

Présentation générale :

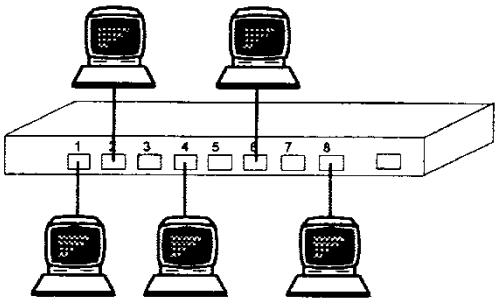
Il existe fondamentalement trois types de « machines » utilisées pour acheminer les données : les **hubs** (« répéteurs » en français, mais personne n'utilise ce mot), les **switchs** (commutateurs en français, même remarque) et les **routeurs**.

Les différents appareils que l'on peut lister comme intervenant dans le câblage d'un réseau se caractérisent par leur niveau d'intervention au niveau des couches réseau



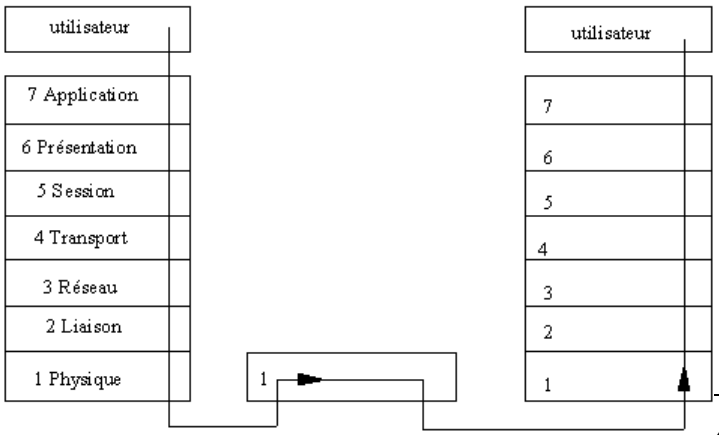
En Câblage avec des paires torsadées, un réseau même minime doit avoir un Hub.

En effet deux ordinateurs ne peuvent être reliés directement entre eux par une liaison UTP. (il faudrait croiser les paires autrement que dans la configuration classique)



Le Hub / Répéteur

Un **Hub** est un amplificateur de signaux qui a au minimum deux connexions réseau. Il travaille sur la **couche 1** du modèle ISO.



Dès qu'il reçoit sur l'une de ses entrées les premiers bits d'une

trame, il la retransmet instantanément sur toutes ses sorties. Un répéteur n'opère aucune modification des données. Les hubs sont souvent utilisés quand il s'agit de relier quelques ordinateurs ensemble pour un petit réseau local. Le principe est simple, dès que quelque chose arrive sur une des prises, il est automatiquement répéter sur toutes les autres prises. C'est pour cela qu'en français, on appelle ça un répéteur...

Sur un hub partagé, toutes les lignes d'entrée (ou au moins toutes les lignes arrivant sur une même carte d'E/S du hub) sont logiquement interconnectées entre elles, constituant ainsi un domaine de collision qui lui est propre. Les règles classiques de la norme 802.3 s'appliquent sur ce hub, y compris l'algorithme de tirage de temps aléatoire ; une seule station à la fois peut transmettre une trame à un instant donné.

Ainsi, dès qu'un ordinateur dit quelque chose, tout le monde l'entend et l'ordinateur concerné traite l'information... C'est pour cette raison que ce système ne peut être utilisé que lorsqu'il n'y a que peu d'ordinateurs, car s'il y a 100 ordinateurs qui parlent en même temps et que tout le monde entend tout ce que tout le monde dit, ça devient vite la … cacophonie !

Deux méthodes existent pour connecter un hub supplémentaire:

- hub "**stand alone**" : Interconnecter des hub au moyen d'un câble

  Dans ce cas, chaque hub à la valeur d'un répéteur selon la règle des répéteurs. (c'est à dire 5 hubs maxi) L'avantage de cette solution réside dans le fait que les répéteurs ne doivent pas se trouver en un voisinage immédiat.

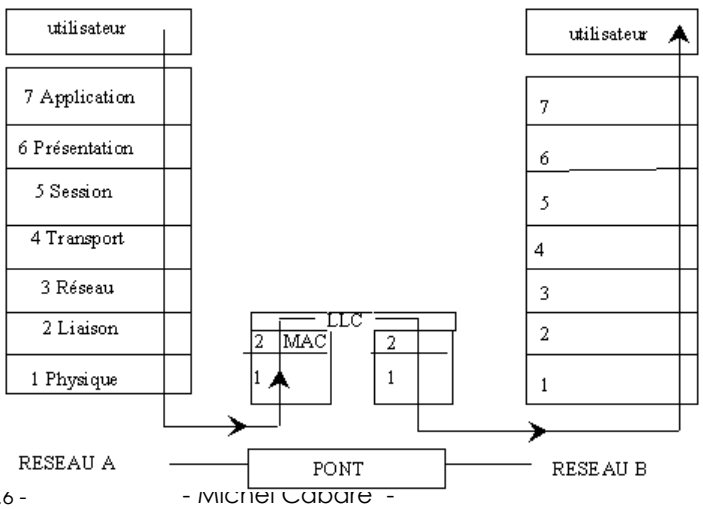
- hub "**empilables**" : Interconnecter les hub à l'aide de ports bus spéciaux et sur des câbles bus très courts.

  L'avantage de cette solution réside dans le fait que tous les répéteurs connectés valent pour un seul hub. on parle alors de hubs empilables

Certains hubs peuvent être aussi équipés d'un module de management. Dans ce cas, on peut piloter ces hubs à distance et effectuer des mesures de trafic et d'erreurs.

Le Switch / Commutateur

Les **switchs** sont un peu plus intelligents. C'est déjà un peu plus gros qu'un hub parce qu'on commence à mettre des choses dedans... Il travaille sur la **couche 2** du modèle ISO.



Il y a toujours ce principe de prises où sont

connectés les différents ordinateurs (mais on peut aussi mettre d'autres switchs, ou des hubs, ou ce que l'on veut...). La différence avec le hub, c'est que le switch sait quels sont les ordinateurs qui sont autour de lui. Ainsi, si il reçoit une trame pour l'ordinateur X, il ne l'envoie qu'à l'ordinateur X et pas aux autres. Il commute (il branche) l'entrée des données vers la sortie où est l'ordinateur concerné. C'est pour cela qu'on appelle ça un commutateur en français...

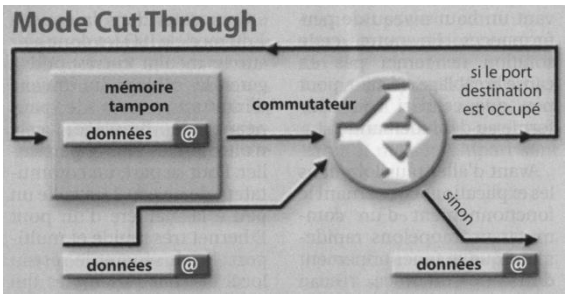
Dans le cas d'un switch, chaque trame arrivant sur une ligne en entrée est mémorisée dans une mémoire tampon interne à la carte d'E/S. Bien que cette façon de faire rende le switch coûteux, elle signifie également que toutes les stations peuvent transmettre et recevoir des trames simultanément. Cela améliore de façon importante les performances globales du système, d'au moins un ordre de grandeur, voire plus. Les trames mémorisées sont ensuite acheminées sur un bus à très haut débit interne au hub, de la carte d'E/S de la station source vers la carte d'E/S de la station destination. Le bus à très haut débit interne au hub n'est pas un produit standardisé, il est le plus souvent spécifique au fabricant de hub.

Lorsque l'on désire augmenter le nombre de noeuds d'un réseau partagé 100Mbits/s et prévenir efficacement les risques de saturation, les switchs sont des équipements incontournables.

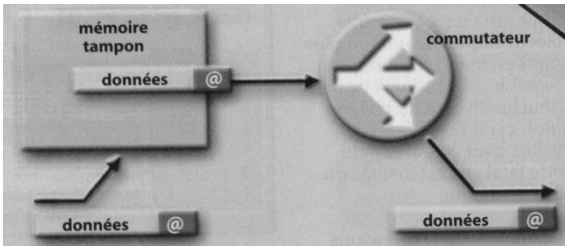
Comment fonctionne un switch ?

Le switch fonctionne en fait comme un pont local multiports. Il permet de scinder un réseau en autant de sous-réseaux qu'il y a de ports. Un switch est nettement plus rapide qu'un pont. Il a deux grands principes généraux de fonctionnement :

1. **"On the fly" dit aussi "Cut Throuhg" :** récupère la trame, analyse les adresses MAC et renvoie si nécessaire sur le port concerné du switch. L'opération est très rapide mais peu sûre (aucun traitement n'est effectué).



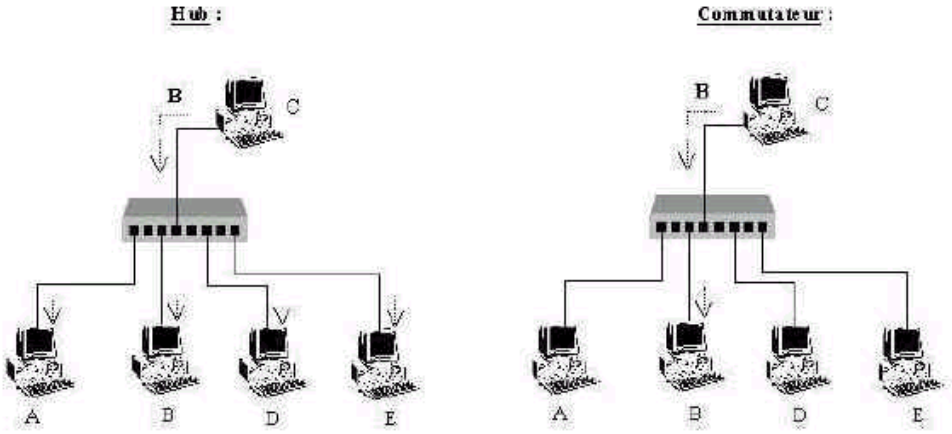
2. **"Store-and-forward" :** stocke la trame en mémoire flash, analyse les adresses MAC et vérifie l'intégrité des données, et renvoie si nécessaire sur le port concerné du switch. C'est une méthode plus lente mais extrêmement sûre concernant la qualité des besoins.



Chaque port d'un switch fait partie d'un seul domaine de collision. Chaque port du switch apprend dynamiquement les adresses MAC (Ethernet) des

équipements qui lui sont connectés. Le switch est capable d'apprendre 1024 ou 2048 adresses par port. (minimum)

Le switch possède un **buffer** circulaire interne travaillant entre 1 ou 2 Gbits/s qui distribue les paquets entrants aux ports de destination s'il y a concordance avec l'adresse apprise dynamiquement par celui-ci.



Routeur :

C'est ce que l'on fait de mieux pour acheminer les données. Le routeur est quasiment un ordinateur à part entière. Il est capable de décoder les trames jusqu'à retrouver l'adresse IP et de diriger l'information dans la bonne direction. On peut aussi définir dans les trames le chemin où doit passer la trame, le routeur peut comprendre tout cela... Le fait de définir ou de diriger une trame s'appelle « router » une trame.

Pont :

Un pont offre la possibilité d'étendre un réseau 802.3-Ethernet-LAN au delà des limites autorisées (nombre de noeuds, longueur maximale, etc...). Les ponts sont de plus en plus utilisés pour contrôler le trafic et la stabilité d'un réseau. Ils travaillent au niveau 2 (couche liaison) du modèle ISO et servent à relier deux réseaux. Cela signifie que les ponts ne doivent pas analyser les paquets (par exemple X25) ou les datagrammes (par exemple IP ou IPX) de la couche réseau, ils doivent simplement se contenter de les insérer dans des trames et de les acheminer. Ils traitent tous les paquets quelque soit leur adresse destination (**Promiscuous Mode**).

Le **taux de défaillance** est réduit, puisque les interférences se produisant d'un côté du pont ne peuvent accéder de l'autre côté. De même, il accroît la **confidentialité**, puisque certaines informations échangées entre des noeuds d'un côté du pont, ne peuvent être "écoutées" de l'autre côté (par exemple les mots de passe échangés entre un serveur et un ordinateur). Enfin, il optimise le **débit**,

puisque des segments séparés par des ponts ont un trafic local qui n'encombre pas le réseau entier.

Les ponts peuvent également relier des segments Ethernet par une ligne synchrone spécialisée, des liaisons satellites, des réseaux commutés et des réseaux en fibre optique (FDDI). En règle générale, ces ponts sont toujours mis en place par paire. Les ponts sont des ordinateurs complets et relativement performants, munis d'une mémoire et d'au moins deux raccords réseau. Ils sont neutres par rapport aux logiciels réseau et peuvent donc fonctionner simultanément avec, par exemple, TCP/IP, IPX, etc...

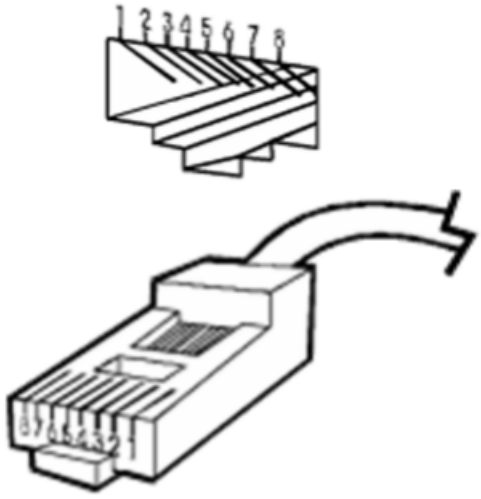
Résumé :

- Les **hubs** ne regardent pas ce qu'il y a dans les trames, ils se contentent de répéter l'information. Il n'y a aucune analyse du contenu de l'information, Ils travaillent au niveau 1 (physique) du modèle OSI.
- Les **switchs** sont capables d'analyser un peu l'information contenue dans la trame, de repérer l'adresse MAC de la destination et d'envoyer la trame vers le bon ordinateur. On dit que les switchs travaillent au niveau 2 du modèle OSI.
- Les **ponts** sont de plus en plus utilisés pour contrôler le trafic et la stabilité d'un réseau. Ils travaillent au niveau 2 (couche liaison) du modèle ISO et servent à relier deux réseaux
- Pour les **routeurs**, retenez simplement qu'ils sont assez puissants et qu'ils travaillent jusqu'au niveau 3 du modèle OSI. Ils sont capable d'analyser le contenu des trames.
- Si les hubs font partie d'un même **domaine de collision**, les switchs, ponts et routeurs permettent de créer des **domaines de collisions séparés**

100 BASE T… EN PRATIQUE

100 Base TX :

Le principe de raccordement est le suivant :



Contact	HUB(MDI-X)	Carte réseau (MDI)
1	RD+ (Réception)	TD+ (Transmission)
2	RD- (Réception)	TD- (Transmission)
3	TD+ (Transmission)	RD+ (Réception)
4	Pas utilisé (masse)	
5		
6	TD- (Transmission)	RD- (Réception)
7	Pas utilisé (masse)	
8		

sur une topologie de câblage en Etoile classique et un schéma de câblage identique au 10 Base T mais nécessitant au minimum de l' **UTP5**

Avec les valeurs maximales admissibles suivantes :

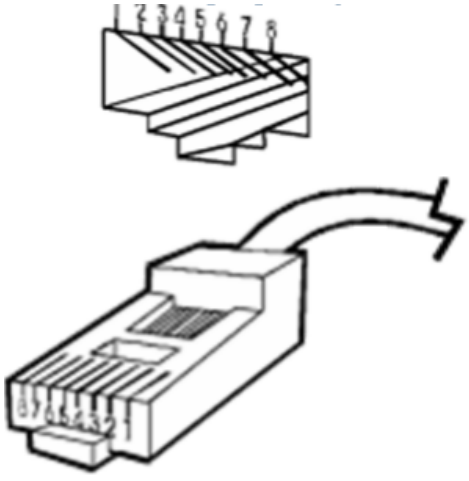
Nombre maxi de segment : 2 / 3 (cf hub classe p **Erreur ! Signet non défini.**)

Longueur maxi Segment : 100 m

Nombre maxi Hub : 1 / 2 (cf hub classe p **Erreur ! Signet non défini.**)

100 Base T4 :

Le principe de raccordement est le suivant :



Contact	HUB(MDI-X)	Carte réseau (MDI)
1	RD+ (Réception)	TD+ (Transmission)
2	RD- (Réception)	TD- (Transmission)
3	TD+ (Transmission)	RD+ (Réception)
4	Bide 4+	Bide 3+
5	Bide 4-	Bide 3-
6	TD- (Transmission)	RD- (Réception)
7	Bide 3+	Bide 4+
8	Bide 3-	Bide 4-

logie de câblage en Etoile classique et un schéma de câblage (identique au 10 Base T mais nécessitant 4 paires dans de l'**UTP3 minimum**)

100 Base FX - SX:

Le principe de raccordement est le suivant, le 100BASE-FX est défini pour fonctionner soit

- Avec 2 brins de fibre optique multimode par lien, un pour la transmission de données, l'autre pour la réception de données. La fibre utilisée est souvent du type (62.5/125) sur une longueur d'onde de 1350 nanomètre.
- Avec 2 brins de fibre optique monomode (SMF) en duplex, fibre de type 9/125.En monomode, la longueur max varie de 10 à 80km suivant la fibre

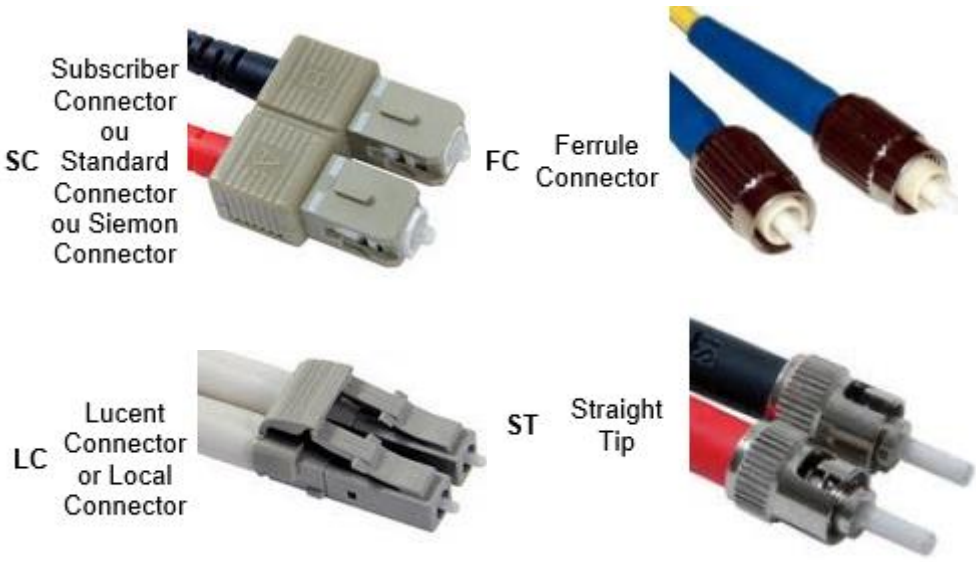
Type de réseau	Débit	Longueur d'onde	OM1 62,5/125	OM 2 50/125	OM3 50/125	OS 1 9/125
100 Base FX	100Mbit/s	1.300nm	5.000 m	5.000 m	5.000 m	

Connecteurs Fibre SC - FC

Une fibre optique peut avoir des connecteurs différents aux 2 extrémités.

Les éléments actifs peuvent avoir une connectique différente mais fonctionner sur le même signal. Il suffit alors de les raccorder avec une fibre mixte. Par exemple : SC d'un côté et LC de l'autre

- Le connecteur le plus fréquent et nommé SC
- Le LC est un petit SC
- Le ST a baïonnette n'est moins utilisé de nos jours.



1000 BASE T… EN PRATIQUE

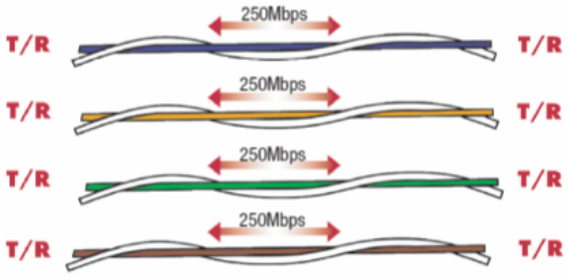
Petite comparaison :

	Ethernet 10BaseT	Fast Ethernet 100BaseT	Prévisions Gigabit Ethernet
Vitesse de transmission de données	10 Mbit/s	100 Mbit/s	1 Gbit/s
Distance maximale sur câble UTP cathégorie 5	100 m	100 m	25 m 100 m (4 paires)
Distance maximale sur câble STP ou coaxial	500 m	100 m	25 m 100 m
Distance maximale sur fibre optique multimode	2 km	412 m en semi-duplex 2 km en duplex intégral	500 m
Distance maximale sur fibre otique monomode	25 km	20 km	2 km

1000 Base TX :

sur une topologie de câblage en Etoile classique et un schéma de câblage identique au 100 Base T sur du RJ45 mais nécessitant au minimum de l' **UTP5e sur 100 m maximum**

Le principe de raccordement est le suivant :

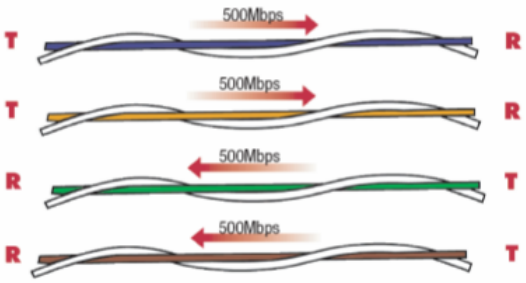


Contact	HUB(MDI-X)	Carte réseau (MDI)
1	BI_D2+	BI_D1+
2	BI_D2-	BI_D1-
3	BI_D1+	BI_D2+
4	BI_D4+	BI_D3+
5	BI_D4-	BI_D3-
6	BI_D1-	BI_D2-
7	BI_D3+	BI_D4+
8	BI_D3-	BI_D4-

Bi_D (Bi Directional Data) signifie données bidirectionnelles suivi du numéro de la paire et du signe électrique.

1000 Base T4 :

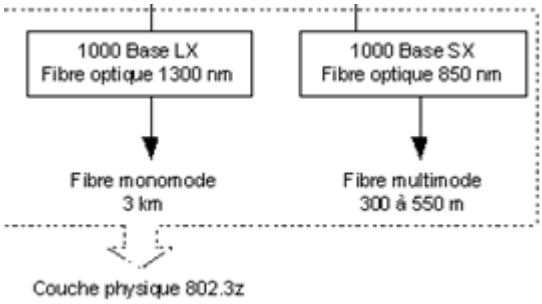
sur une topologie de câblage en Etoile classique et un schéma de câblage identique au 100 Base T sur du RJ45 mais nécessitant au minimum de l' **UTP6 sur 100 m maximum**



Contact	HUB(MDI-X)	Carte réseau (MDI)
1	RX 1	TX 1
2	RX 1	TX 1
3	TX 1	RX 1
4	RX 2	TX 2
5	RX 2	TX 2
6	TX1	RX 1
7	TX 2	TX 2
8	TX 2	TX 2

1000 Base Fibre Lx - Sx:

On pourra utiliser 2 types de fibre



- Avec 2 brins de fibre optique multimode avec 2 longueurs d'onde longueur d'onde de 850 et 1300 nanomètre et 3 types de fibre
- Avec 2 brins de fibre optique monomode (SMF) en duplex, fibre de type 9/125.En monomode, la longueur max est de 5 km suivant la fibre

Type de réseau	Débit	Longueur d'onde	OM1 62,5/125	OM 2 50/125	OM3 50/125	OS 1 9/125
1000 Base SX	1Gbit/s	1.300nm	275 m	550 m	550 m	
1000 Base LX	1Gbit/s	1.200nm	550 m	550 m	550 m	

Connecteurs Fibre SC - FC

Une fibre optique peut avoir des connecteurs différents aux 2 extrémités.

Les éléments actifs peuvent avoir une connectique différente mais fonctionner sur le même signal. Il suffit alors de les raccorder avec une fibre mixte. Par exemple : SC d'un côté et LC de l'autre. Les différents types sont identiques à ceux présentés pour le 100BaseF

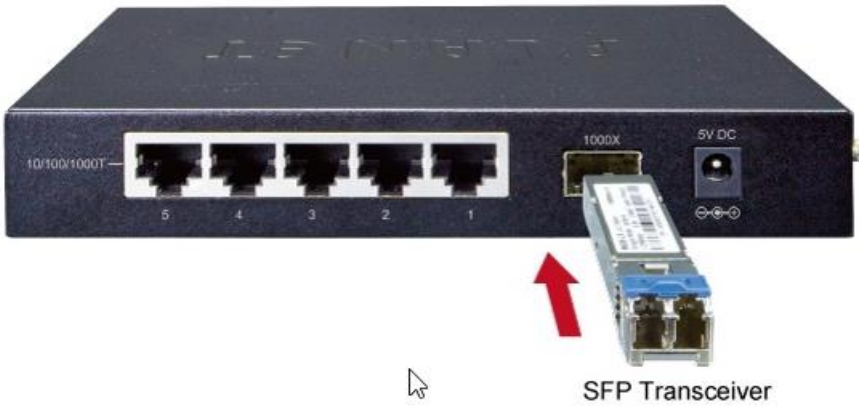
Connecteur SFP

Les **Connecteur SFP** pour **small form-factor pluggable** sont conçus pour supporter SONET, Gigabit Ethernet, Fibre Channel, et beaucoup d'autres standards de communication, y compris la paire cuivrée. En raison de sa petite taille, le SFP rend obsolète l'ancien et très répandu Gigabit Interface Converter (GBIC), et il est parfois appelé mini-GBIC

Ces connecteurs permettent une souplesse dans le type de signal souhaité, car ils sont interchangeables et permettent donc de changer le type de signal optique en changeant uniquement le module optique (petit et moins cher)

Connecteur signés – génériques :

Les formats des transceivers SFP, ont été standardisés par des accords entre fabricants de telle sorte que les dimensions, les connecteurs et les signaux sont homogènes et interchangeables. Prenez garde néanmoins que certaines grandes marques, notamment Cisco, vendent des équipements réseau dont les logements n'acceptent pas les transceivers d'autres marques…



DAC – Direct Attach Cable

Câble propriétaire pour Relier 2 connecteurs SFP Câble propriétaire pour Relier 2 connecteurs

Le câble DAC peut être divisé en actif et passif.

- Actif L'ensemble émetteur-récepteur à fibre optique du câble DAC actif est équipé de composants électriques, et augmente la distance de transmission (maxi 10-12m) mais son prix est également plus élevé.
- Passif il peut transmettre un signal optique sans utilisation d'énergie électrique. Moins loin (maxi 3-5 m)

10G BASE T… EN PRATIQUE

10G Base T :

Sur une topologie de câblage en Etoile classique et un schéma de câblage identique au 100 Base T sur du RJ45 mais nécessitant au minimum de l' **STP6 4 paires sur 100 m maximum**

Attention, les Vitesses de replis standards sur un Hub Switch 10 avec une carte non 10G est de 1G, même si le câble est capable de faire "passer plus".

Speed	Compatible Cable
10G	CAT6a (100m)
	CAT6 (55m)
	CAT5e (30m)
5G	CAT6 (100m)
	CAT5e (30m)
2.5G	CAT5e (100m)

5G Base T - 2.5G base T

Si maintenant on a un appareil qui accepte les dernières Normes "intermediaires" récentes, que sont les :

- 5G Base T et la
- 2.5G Base T,

alors selon les câble, on peut avoir un débit qui s'ajustera au mieux !

10G Base "fibre:

On pourra utiliser plusieurs types de normes, parmi lesquelles les principales étant 10G base S (10Gbase SR), 10G base L, 10G base LX4 et 10GbaseE

- Avec 2 brins de fibre optique multimode avec 2 longueurs d'onde et 4 types de fibre, La longueur max est de 300 a 500m suivant la fibre
- Avec 4 brins de fibre optique monomode (SMF) en duplex, 2 fibres de type 9/125. La longueur max est de 10 a 40 km suivant la fibre

Type de réseau	Débit	Longueur d'onde	OM1 62,5/125	OM 2 50/125	OM3 50/125	OS 1 9/125
10G Base S	10Gbit	850nm	30 m	82 m	300 m	-
10G Base L	10Gbit	1.310nm	-	-	-	10.000 m
10G Base LX4	10Gbit	1.310nm	300 m	300 m	300 m	10.000 m
10G Base E	10Gbit	1.500nm	-	-	-	40.000 m

Les type de Fibre OS1 - OS2 -OM1 - OM2 - OM3 - OM4…

Fibre	Type	Dimensions (micron)	Largeur de bande OFLBW (850 nm-1 300 nm)	Largeur de bande RML (850 nm)
OM1	Multimode	62,5 / 125	200-500 MHz•km	Non spécifié
OM2	Multimode	50 / 125	500-500 MHz•km	Non spécifié
OM3	Multimode	50 / 125	1 500-500 MHz•km	2 000 MHz•km
OM4	Multimode	50 / 125	3 500-500 MHz•km	4 700 MHz•km
OS1	Monomode	9 / 125	> 10 GHz•km (non spécifié)	> 10 GHz•km (non spécifié)
OS2	Monomode	9 / 125	> 10 GHz•km (non spécifié)	> 10 GHz•km (non spécifié)

Il y a même une couleur officielle pour chaque Fibre

Modes	Couleurs de la gaine	Diamètres de la fibre	Applications principales
OM1	Orange	62.5/125µm	Connections moyennes distances
OM2	Orange	50/125µm	Connections moyennes distances
OM3	Aqua	50/125µm	Connections moyennes distances réseaux Gigabit et Datacenter
OM4	Aqua	50/125µm	Datacenter

Mode	Couleur de la gaine	Diamètre de la fibre	Applications principales
OS1/2	Jaune	9/125µm	Connections longues distances ou à débit élevé

Quelle fibre selon débit escompté et distance

Ne sont pas mentionnées ici les fibres OS (monomodes) car leur Cout / portée les exclus pratiquement des Usages LAN. Donc ce tableau affiche les valeurs courantes pour les fibres multi Modes

Protocole	Débit	Source	OM1	OM2	OM3	OM4
100BaseFX	100 Mb/s	LED @ 850 nm	5 000 m	5 000 m	5 000 m	5 000 m
1000BaseSX	1 Gb/s	VCSEL @ 850 nm	275 m	550 m	1 000 m	1 100 m
1000BaseLX	1 Gb/s	LASER @ 1 300 nm	550 m	550 m	550 m	600 m
10G BaseSR	10 Gb/s	VCSEL @ 850 nm	33 m	82 m	300 m	550 m
10G BaseLX4	10 Gb/s	CWDM @ 1 300 nm	300 m	300 m	300 m	300 m
10G BaseLRM	10 Gb/s	LASER @ 1 300 nm	220 m	220 m	220 m	220 m
40G BaseSR4	40 Gb/s	VCSEL @ 850 nm	NA	NA	100 m	125 m
100G BaseSR10	40 Gb/s	VCSEL @ 850 nm	NA	NA	100 m	125 m

10GBaseS = 10GbaseSR

Connecteurs Fibre SC - FC

Une fibre optique peut avoir des connecteurs différents aux 2 extrémités.

Les éléments actifs peuvent avoir une connectique différente mais fonctionner sur le même signal. Il suffit alors de les raccorder avec une fibre mixte. Par exemple : SC d'un côté et LC de l'autre

Les différents types sont identiques à ceux présentés pour le 100BaseF

Connecteur SFP+

SFP+ pour **enhanced small form-factor pluggable** est une version améliorée du SFP. Il garde le même format, mais il supporte un débit de données plus élevé, jusqu'à 10 gigabits par seconde.

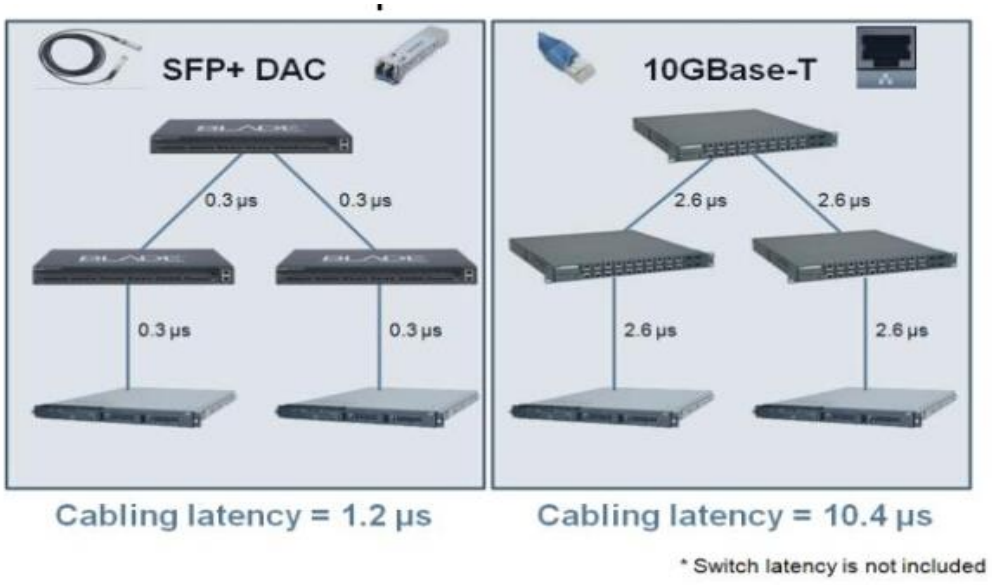
La norme SFP+ a été publiée pour la première fois le 9 mai 2006 et la version 4.1 a été publiée le 6 juillet 2009. SFP+ supporte le Fibre Channel jusqu'à 8 gigabits par seconde, 10 gigabits par seconde Ethernet

Un slot SFP+ peut être conçu de façon à accepter un module SFP standard. Il y a donc possibilité de rétro-compatibilité entre SFP+ et SFP.

DAC – Direct Attach Cable

Câble propriétaire pour Relier 2 connecteurs SFP+, s'il permet d'améliorer la latence, il ne permet pas en général de longue distance (entre 1 et 8 m)

N.B: En 10G Consomme beaucoup moins d'électricité que la paire cuivrée (et donc dégage moins de chaleur)

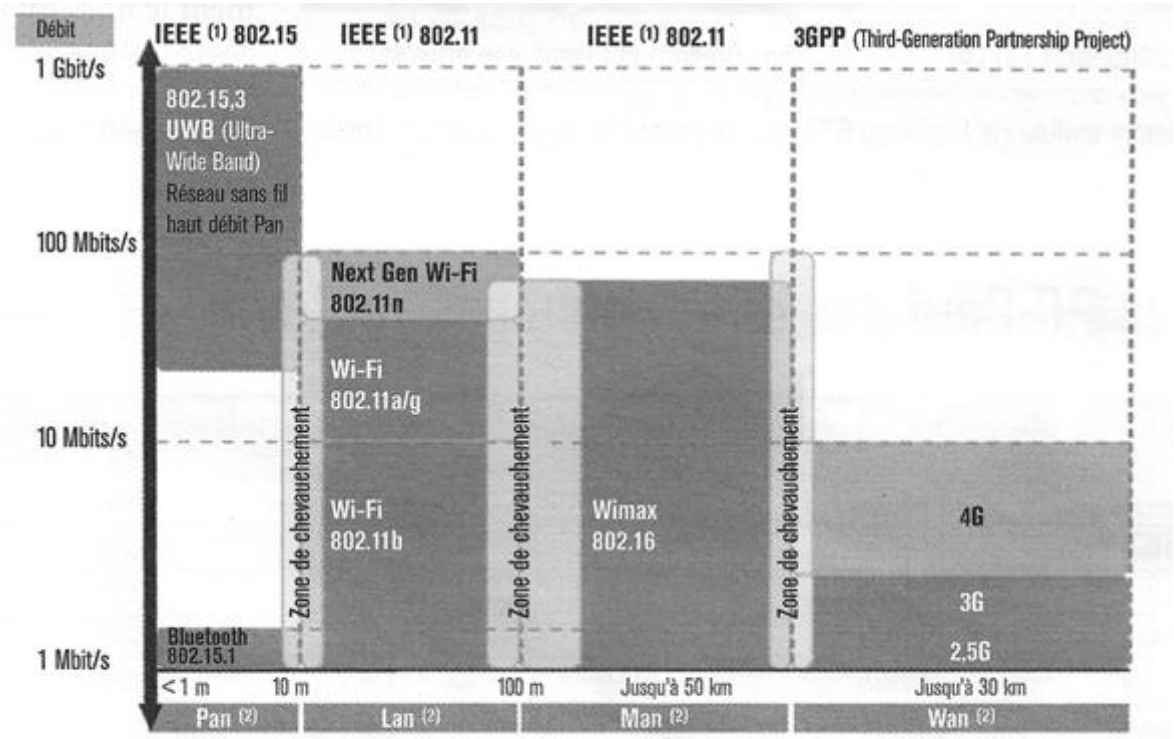


RESEAUX SANS FILS

Présentation:

Dans les technologies mobiles ont peut discerner :

- Les **WPAN** (**Wireless Personal Area Network**) : avec des marques telles que Bluetooth, HomeRF
- Les **WLAN** (**Wireless Local Area Networks**) : avec deux standards principaux, IEEE 802.11 (US) sur des ondes radio 2.4 Ghz ou 5Ghz avec un débit symétrique de 50Mbit/s sur 100m et Hiperlan (Europe)
- Le **WMAN** (**Wireless Metropolitan Area Networks**) ou **Wimax** qui est une sorte de WIFI longue portée basée sur des ondes radio 3.5Ghz avec un débit symétrique de 75Mbit/s sur 50km
- Les technologies cellulaires (**GSM**, **GPRS**, **UMTS**)



(1) Institute of Electrical and Electronics Engineers. (2) Pan : Personal Area Network, ou réseau personnel ; Lan : Local Area Network ou réseau local ; Man : Metropolitan Area Network ou réseau métropolitain ; Wan : Wide Area Network ou réseau étendu. Source : www.intel.com

Dans le spectre de la WIFI, 2 technologies principales:

- Une **WPAN** (**Wireless Personal Area Network**) : avec la norme **Bluetooth** lancée à l'origine en 1994 par Ericsson qui touche le domaine de la domotique. Après une première spécification en 1999 puis une deuxième en 2004, travaille à 2.4 GHz soit la même bande que le WI-FI

  1Mb/s Full Duplex,puis 10Mb/S en 2004, portée de 10 m (1 mW)

- Une **WLAN** (**Wireless Local Area Networks**) : avec le standard principal, **802.11** ou **WIFI** de l'IEEE sera traité dans un chapitre spécifique.

Ces 2 protocoles ne sont absolument pas compatibles entre eux.

RESEAUX SANS FILS ET ARCEP

ARCEP Autorité de Régulation Communication Electronique et des Postes:

http://www.arcep.fr

…la bande 5 GHz est également ouverte aux systèmes Wi-Fi dans un cadre spécifique. La décision n° 2008-0568 de l'ARCEP autorise ainsi les systèmes Wi-Fi à fonctionner dans les fréquences 5250-5350 MHz et 5470-5725 MHz, en imposant la mise en œuvre d'un mécanisme de sélection dynamique de fréquences (DFS) et un mécanisme de régulation de la puissance de l'émetteur. Ces modalités sont nécessaires afin de garantir un fonctionnement compatible avec les autres systèmes radars utilisant ces bandes de fréquences… (armées, protection civile)

Wifi – déclaration ou non:

Par " opérateur ", on entend toute personne physique ou morale qui exploite un réseau de communications électroniques ouvert au public ou qui fournit au public un service de communications électroniques (art. L.32 du code des poste et des communications électroniques).

Le tableau synthétique des acteurs soumis à l'obligation de déclaration

Le périmètre des acteurs soumis à l'obligation de déclaration (article D. 98 du CPCE)

<table>
<tr><th colspan="3">Les réseaux utilisant des fréquences libres d'usage</th></tr>
<tr><th colspan="2">Réseaux ouverts au public</th><th>Réseaux n'étant pas ouverts au public</th></tr>
<tr><td>Réseaux ouverts au public</td><td>Réseaux internes ouverts au public
(ex : cybercafés, hôtels ou toute
offre de service à partir d'une borne connectée à un réseau déjà déclaré)</td><td>Réseaux indépendants (ex : réseau d'entreprises)
Réseaux privés</td></tr>
<tr><td>Doivent se déclarer à l'ARCEP</td><td colspan="2">Ne doivent pas se déclarer à l'ARCEP</td></tr>
</table>

- Un réseau est " ouvert au public " dès lors qu'il est établi ou utilisé pour fournir des " services de communication au public par voie électronique " à l'attention du public

L'absence de déclaration Arcep

- Un réseau Wi-Fi localisé à un bâtiment ou une zone réduite rentre dans cette qualification de « réseau interne ouvert au public ». (cybercafés, bureaux, hôtels, bibliothèque. Le mode d'accès au réseau (filaire ou hertzien) autant que le nombre de personnes pouvant se connecté n'a pas d'influence tant que le réseau reste localisé. Il faut uniquement que ce public soit restreint !

Puissance des canaux - Pire

Tout cela est réglementé bien évidemment par l'Arcep…"*Il résulte de la limitation sur la puissance (PIRE) que l'étendue d'un réseau constitué au moyen de la seule technologie RLAN est typiquement de quelques centaines de mètres. L'opérateur qui souhaite déployer des liaisons point à point, avec des portées non compatibles avec les limitations de puissance indiquées dans les tableaux, doit solliciter à cet effet auprès de l'Autorité une autorisation d'utilisation de fréquences dans l'une des bandes de fréquences identifiées pour cet usage*"

Les puissances sont exprimées en **PIRE** : **puissance isotrope rayonnée équivalente**

Sur la bande des 2.4 Ghz

Dans tous les départements métropolitains :

<table>
<tr><th>Fréquences en MHz</th><th>Intérieur</th><th>Extérieur</th></tr>
<tr><td>2400
2454</td><td rowspan="2">100 mW</td><td>100 mW</td></tr>
<tr><td>2483,5</td><td>10 mW</td></tr>
</table>

Sur la bande des 5 Ghz

En extérieur et en intérieur

Bandes de fréquences	Limite de PIRE moyenne maximale autorisée	Densité de PIRE moyenne maximale autorisée	Techniques d'atténuation
Bande 5470-5725 MHz	1 W avec une régulation de la puissance de l'émetteur* 500 mW sans régulation de la puissance de l'émetteur*	50 mW/MHz dans toute bande de 1 MHz avec une régulation de la puissance de l'émetteur* 25 mW/MHz dans toute bande de 1 MHz sans régulation de la puissance de l'émetteur*	Obligation de mettre en place les techniques d'atténuation**

En intérieur uniquement

Bandes de fréquences	Limite de PIRE moyenne maximale autorisée	Densité de PIRE moyenne maximale autorisée	Techniques d'atténuation
Bande 5150-5250 MHz	200 mW	0,25 mW dans toute bande de 25 kHz	pas d'obligation
Bande 5250-5350 MHz	200 mW avec une régulation de la puissance de l'émetteur* 100 mW sans régulation de la puissance de l'émetteur*	10 mW/MHz pour toute bande de 1 MHz avec une régulation de la puissance de l'émetteur* 5 mW/MHz pour toute bande de 1 MHz sans régulation de la puissance de l'émetteur*	Obligation de mettre en place les techniques d'atténuation**

Obligation "légales"

Que l'on soit déclaré ou non, tout réseau WIFI accessible au Public doit normalement respecter un certain nombre d'obligations

L'accès Internet est, en France, est soumis à un cadre précis :

- identification de l'utilisateur (assez controversé)
- conservation temporaires de ses données de connexion (obligatoire)
- filtrage des contenus illicites (tres controversé)

font partie des principales règles à mettre en place. Sans ce passage obligé, les entreprises se mettent en porte-à-faux avec la loi.

- identification de l'utilisateur (non obligatoire)

La contrainte de traçabilité des usagers pourrait faire croire à la nécessitée d'imposer l'identification de chaque utilisateur (par exemple, par un identifiant et un mot de passe associé), avant tout accès

mais, le décret du 24 mars 2006 n'a pas retenu l'hypothèse consistant à demander aux exploitants de « cybercafés », d'hôtels ou de bars qui offrent une connexion Wi-Fi, de relever l'identité de leurs clients. Il prévoit seulement la conservation des « données permettant l'identification ». Il s'agit donc, pour ces « fournisseurs de Wi-Fi » de recueillir des informations qui, mises bout à bout, constituent un faisceau d'indices permettant l'identification

- conservation temporaires de ses données de connexion (obligatoire)

Les organismes qui mettent à disposition du public un service de libre accès à internet (postes informatiques, wi-fi, etc.) sont considérés comme opérateurs de communications électroniques (OCE) et sont soumis aux obligations prévues àl'article L. 34-1 du code des postes et des communications électroniques(CPCE). A ce titre, ils doivent conserver les données de trafic répondant aux " besoins de la recherche, de la constatation et de la poursuite des infractions pénales " et destinées aux autorités légalement habilitées.

La plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie.

Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement (Article R. 10-13 du Code des postes et des communications électroniques)

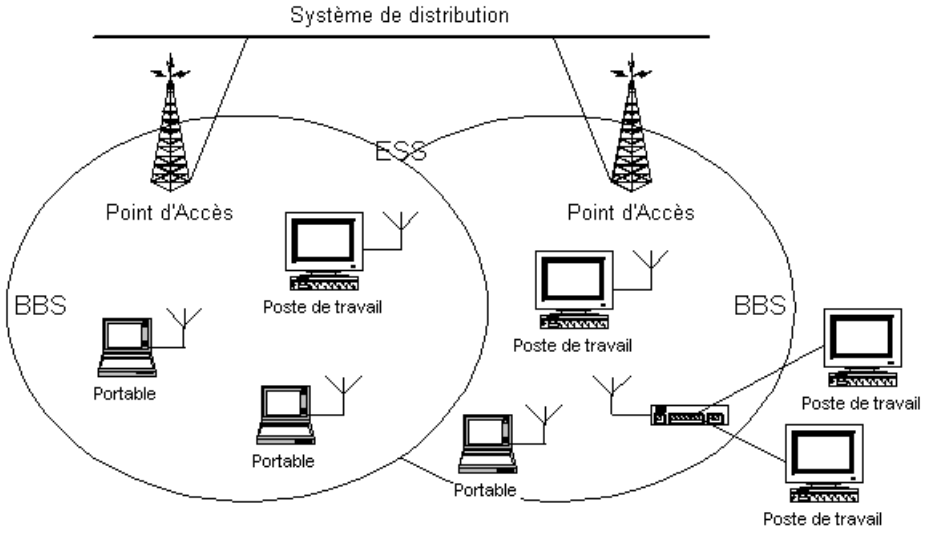
- filtrage des contenus illicites (aucune obligation)

LES LIAISONS WI-FI

Structure des liaisons:

En 1998, la norme **802.11** est finalisée, et est rapidement rebaptisée **Wi-Fi (Wireless fidelity**). Un organisme, la **WECA (Wireless Ethernet Compatibility Alliance)**, s'est donné la mission de certifier l'inter-opérabilité des produits avec la norme 802.11b

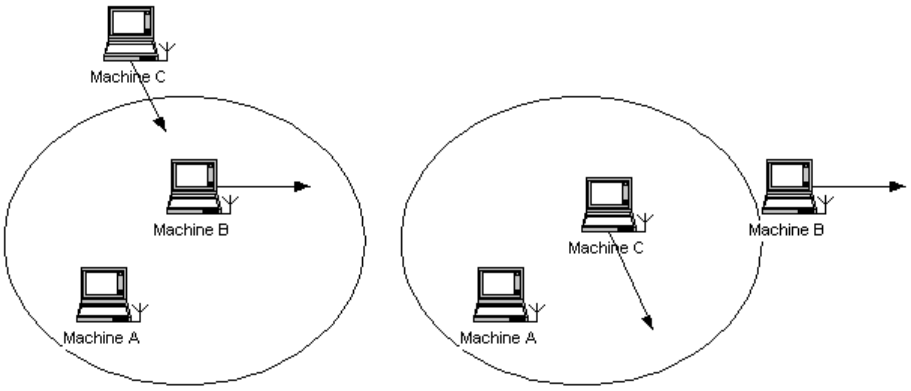
Cette norme est basée sur une architecture cellulaire (le système est subdivisé en cellules), et où chaque cellule (appelée **Basic Service Set** ou **BSS** dans la nomenclature 802.11), est contrôlée par une station de base (appelée **Access Point** ou **AP**, Point d'Accès en français).



deux modes principaux de fonctionnement existent pour les liaisons sans fils.

Fonctionnement "AD-HOC" (IBSS):

Un réseau **Ad Hoc** est un réseau où il n'y a pas d'infrastructures fixes.

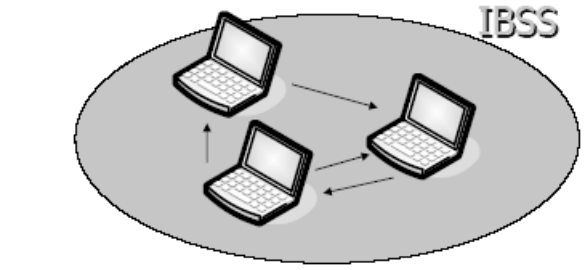


Le signal est transmis par l'intermédiaire des mobiles présents et routé dynamiquement. Une partie de ses fonctionnalités sont reprises par les stations

elles-mêmes mais alors certaines fonctions ne sont pas utilisables (comme le mode d'économie d'énergie).

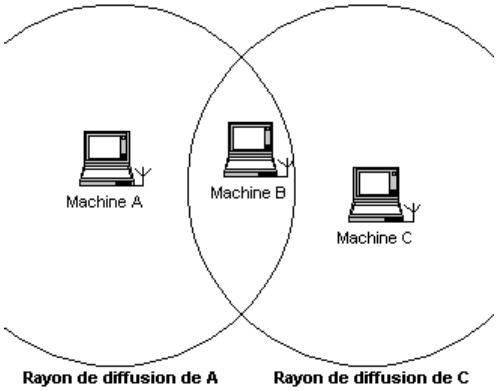
Ceci peut permettre le transfert de fichiers entre deux utilisateurs..

on parle aussi de **Mode IBSS**



Independant Basic Service Set

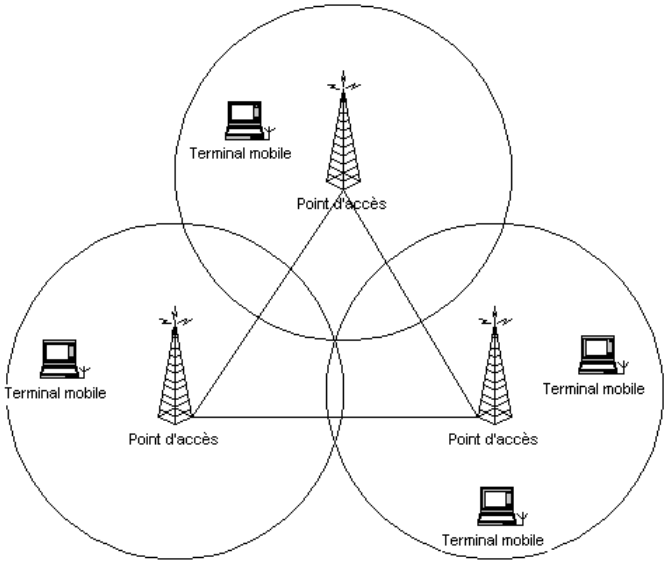
Dans une connexion ad hoc, il n'y a pas de possibilité de transfert entre les machines distantes, autres que les deux qui ont initié la communication.



Dans le schéma ci-dessus, la machine A peut dialoguer avec la machine B, mais pas avec la machine C

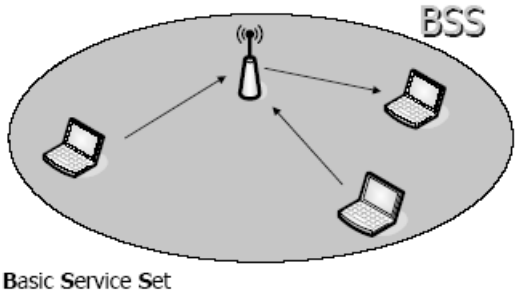
Fonctionnement "Infrastructure":

Le mode **infrastructure** fait appel a une ou plusieurs bornes de concentration appelées **Points d'Accès**, qui gère l'ensemble des communications dans une même zone géographique.



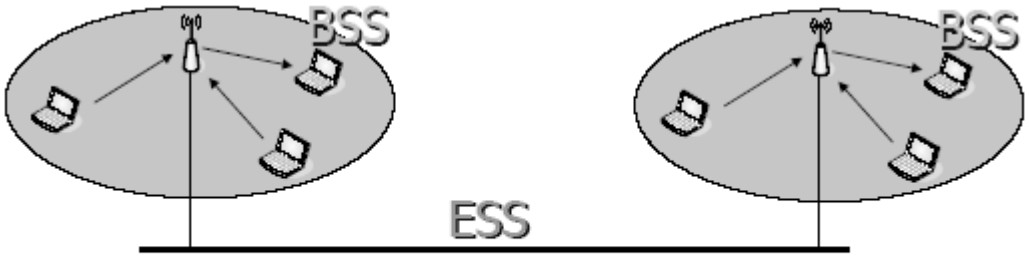
Les bornes sont connectées entre elles par une liaison ou un réseau filaire ou hertzien.

on parle aussi de **Mode IBSS**



Basic Service Set

On parle également de points d'accès en mode "Pont" voire **Mode ESS**



Extended Service Set ID

Comment une station rejoint-elle une cellule existante ?

Quand une station veut accéder a un **BSS** existant (soit après un allumage, un mode veille, ou simplement en entrant géographiquement dans la zone de

couverture de la cellule), la station a besoin d'informations de synchronisation de la part du Point d'Accès.

La station peut avoir ces informations par un des deux moyens suivants :

1. **Ecoute passive** : dans ce cas, la station attend simplement de recevoir une trame balise (**Beacon Frame**). La trame balise est une trame envoyée périodiquement par le Point d'Accès contenant les informations de synchronisation.
2. **Ecoute active** : dans ce cas, la station essaie de trouver un Point d'Accès en transmettant une trame de demande d'enquête (**Probe Request Frame**) et attend la réponse d'enquête du Point d'Accès.

Ces deux méthodes sont valables et peuvent être choisies en fonction des performances ou de la consommation engendrées par l'échange, en terme d'énergie.

Le processus d'authentification

Une fois qu'une station a trouvé un Point d'Accès et a décidé de rejoindre une cellule (BSS), le processus d'authentification s'enclenche. Celui-ci consiste en l'échange d'informations entre le Point d'Accès et la station, où chacun des deux partis prouve son identité par la connaissance d'un certain mot de passe.

Le processus d'association - réassociation

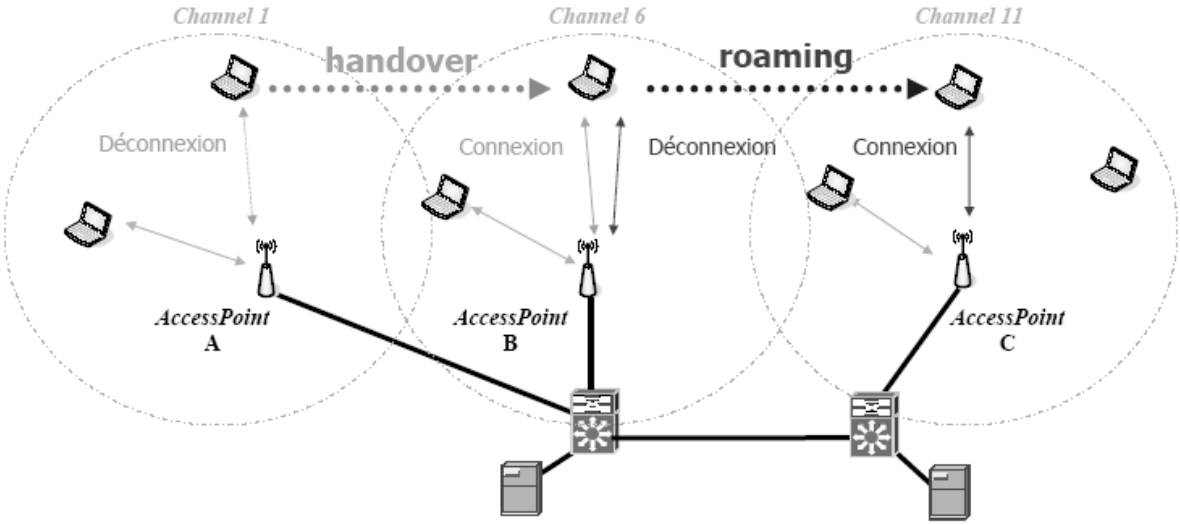
Une fois la station authentifiée, le processus d'association s'enclenche. Celui-ci consiste en un échange d'informations sur les différentes stations et les capacités de la cellule, et autorise le DSS (les Points d'Accès enregistre la position actuelle de la station). Seulement après le processus d'association, la station peut transmettre et recevoir des trames de données.

La réassociation peut survenir à cause d'éloignement grandissant, ou de gestion de la répartition de charge.

Le roaming- handover

Les terminaux BSS peuvent se déplacer au sein de la cellule et garder une liaison directe avec le point d'accès AP, ou changer de cellule, ce qui s'appelle le **roaming**

Pour un réseau **Wi-Fi**, ce terme est utilisé pour évoquer le fait d'un changement de cellule ou de réseau tout en restant en communication (voix ou données). Dans ce cas il s'agit en fait plus d'un **Handover** que d'un **roaming**



En TCP-IP, (qui est basé sur des paquets), la transition d'une cellule à une autre se fait entre deux transmissions de paquets, (contrairement à la téléphonie où la transition peut subvenir au cours d'une conversation.) Ceci rend le roaming plus facile en théorie, mais… les performances seront considérablement réduites à cause de la retransmission qui sera exécutée par les protocoles des couches supérieures.

Le standard 802.11 ne définit pas comment le roaming est fait, mais en définit cependant les règles de base. (l'écoute active ou passive, le processus de ré-association, où une station qui passe d'un Point d'Accès à un autre sera associée au nouveau Point d'Accès).

Sécurité

La sécurité est le premier (ou le dernier !) soucis de ceux qui déploient les réseaux locaux sans fil. Le comité de 802.11 a apporté une solution en élaborant un processus appelé **WEP** (**Wired Equivalent Privacy**).

Le principal, pour les utilisateurs, est d'être sûr qu'un intrus ne pourra pas :

Accéder aux ressources du réseau (prévenir l'accès non authentifié)

Ceci est obtenu en utilisant un mécanisme d'authentification où une station est obligée de prouver sa connaissance d'une clef, ce qui est similaire à la sécurité sur réseaux câblés, dans le sens où l'intrus doit entrer dans les lieux (en utilisant une clef physique) pour connecter son poste au réseau câblé.

Capturer le trafic du réseau sans fil (Ecoute clandestine)

L'écoute clandestine est bloquée par l'utilisation de l'algorithme **WEP** qui est un générateur de nombres pseudo aléatoires initialisé par une clef secrète partagée. Basé sur l'algorithme RC4 de RSA (faible sécurité)

L'économie d'énergie

Les réseaux sans fil sont généralement en relation avec des applications mobiles, et dans ce genre d'application, l'énergie de la batterie est une ressource importante. C'est pour cette raison que le standard 802.11 donne lui-même des directives pour l'économie d'énergie et définit tout un mécanisme pour permettre aux stations de se mettre en veille pendant de longues périodes sans perdre d'information. L'idée générale, est que le Point d'Accès maintient un enregistrement à jour des stations travaillant en mode d'économie d'énergie, et garde les paquets adressés à ces stations jusqu'à ce que les stations les demandent avec une **Polling Request**, ou jusqu'à ce qu'elles changent de mode de fonctionnement.

NORMES ETHERNET 802.11 …

Panels des Normes 802.11

Protocole	Date de normalisation	Fréquences	Taux de transfert (Typ)	Taux de transfert (Max)
Norme initiale	1997	2,4-2,5 GHz	1 Mbit/s	2 Mbit/s
802.11a	1999	5,15-5,35 GHz 5,47-5,725 / 5,725-5,875	25 Mbit/s	54 Mbit/s
802.11b	1999	2,4-2,5 GHz	6,5 Mbit/s	11 Mbit/s
802.11g	2003	2,4-2,5 GHz	25 Mbit/s	54 Mbit/s
802.11n	2009	2,4 GHz et/ou 5 GHz	200 Mbit/s	450 Mbit/s
802.11ac	jan. 2014	5,15-5,35 GHz 5,47-5,875 GHz	433 Mbit/s[1]	1300 Mbit/s

Les anciens 802.11a – 802.11b et 802.11g :

802.11b en 1999 – label WI-FI

la norme **802.11b** ou **802.11HR** (High Rate), dans la bande 2,4 GHz normalisée en septembre 1999. La technologie **DSSS** est gardée.

- Débits de 11 Mbps,
- portée de 30-50 mètres. (1 Mbps 250 m)
- Canaux disponibles (non recouvrant) : 3 parmi 13
- La Sécurité (faible) est obtenue par codage **WEP**

Une variante est connue sous la norme **802.11b+** Débits de 22 Mbps

802.11a en 1999

la norme **802.11a** , opérant dans la bande des 5 à 5.8 GHz, (moins encombrées que celle de 2.4Ghz) met l'accent sur l'utilisation de la technologie **OFDM** au niveau physique pour atteindre des débits plus élevés et une meilleure immunité aux interférences. Par contre il est plus sensible aux obstacles naturels et physiques(béton armé)…

- Débits de 54 Mbps
- portées de 50 mètres. !
- Canaux disponibles (non recouvrant) : 8

N.B : Il est donc incompatible avec les standards **802.11b et 802.11b+**

802.11g en 2003

la norme **802.11g**, bande 2,4 GHz et 5 GHz

- Débits de 54 Mbps
- Portée de 100 mètres.
- Canaux disponibles (non recouvrant) : 3 parmi 13
- La Sécurité est obtenue par la norme **802.i et autres 802.x**

N.B : Il est donc compatible avec les standards **802.11b (et 802.11b+)**

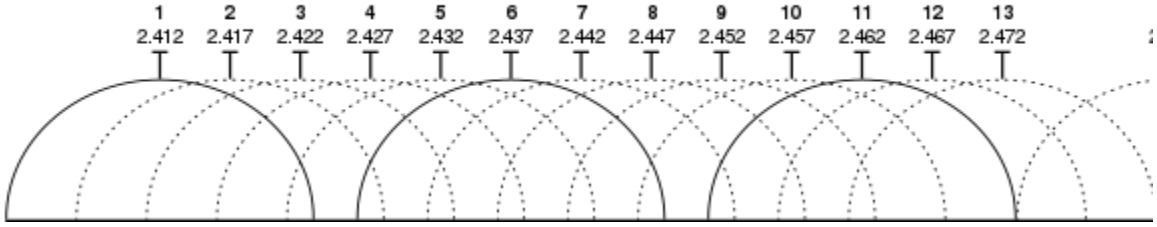
N.B : mais la compatibilité entre les standards **802.11b /g « coute cher »**, car il suffit qu'un seul point se connecte en b pour que la borne fasse passer son débit de 54 à 11 Mbps

Bande 2.4 Ghz - gestion des 13 canaux 802.11b-g partage de charge

Le choix des fréquences utilisables dépends bien évidemment du pays dans lequel on se trouve, il existe à cet effet une normalisation internationale

A ce propos, si le paramétrage des bornes demande toujours de choisir une régionalisation ! Cela va bien au-delà de la langue d'affichage des menus !

N.B: 2 Bornes avec une régionalisation différente risquent de ne pas pouvoir communiquer entre elles du fait de l'utilisation de fréquences différentes.



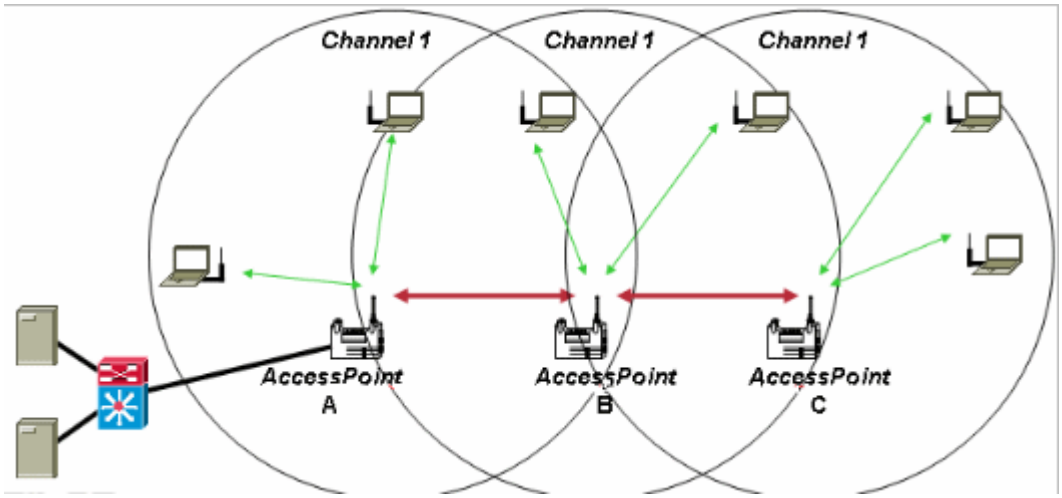
En résumé on pourrait faire le tableau suivant :

802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
a	5 GHz	54 Mbps	Faible	Faible	20 MHz	Non
b	2,4 GHz	11 Mbps	Correcte	Elevée	20 MHz	Non
g	2,4 GHz	54 Mbps	Correcte	Elevée	20 MHz	Non

	802.11b (alias Wi-Fi)	802.11a (alias Wi-Fi5)	802.11g
Norme validée par l'IEEE*	Oui	Oui	Oui
Date d'introduction	1999	2003	2003
Bande de fréquences	2,4 GHz	5 GHz	2,4 GHz
Débit théorique maximal	11 Mbits/s	54 Mbits/s	54 Mbits/s
Débit effectif à une distance de 2 à 18 m	4 à 6 Mbits/s	4 à 20 Mbits/s	4 à 20 Mbits/s
Distance théorique maximale à l'intérieur	45 m	22 m	45 m
Nombre de canaux "non recouvrants"	3	8	3

Pour optimiser la présence de différents AP pour couvrir une même zone, il faut savoir que au-delà de 3 éléments, c'est inutile (car il y aura télescopage des fréquences).

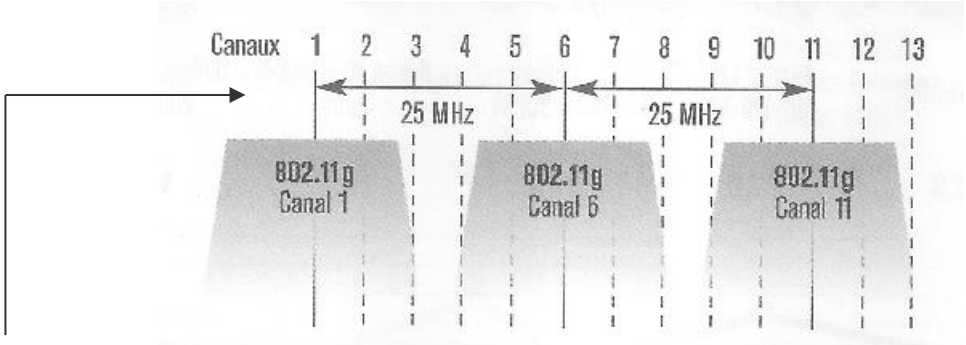
3 points d'accès en mode répéteur sur une zone de couverture partagent un débit atteignant au maximum le débit nominal d'une borne.



Mais 3 points d'accès sur une zone de couverture peuvent donner un débit atteignant de 33Mbits/s en utilisant un plan de fréquence approprié

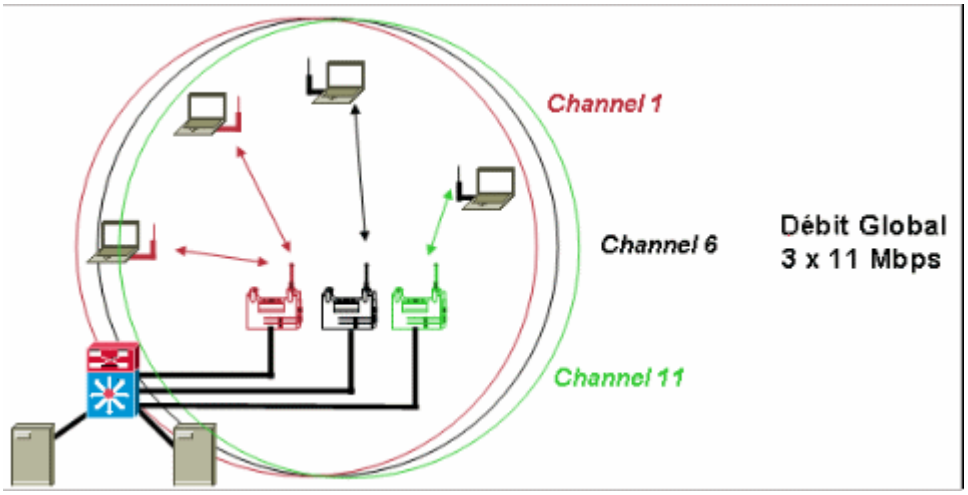
1/6/11 – 2/7/12 – 3/8/13, et 5/10

(Voire en France **1/5//9/13)**

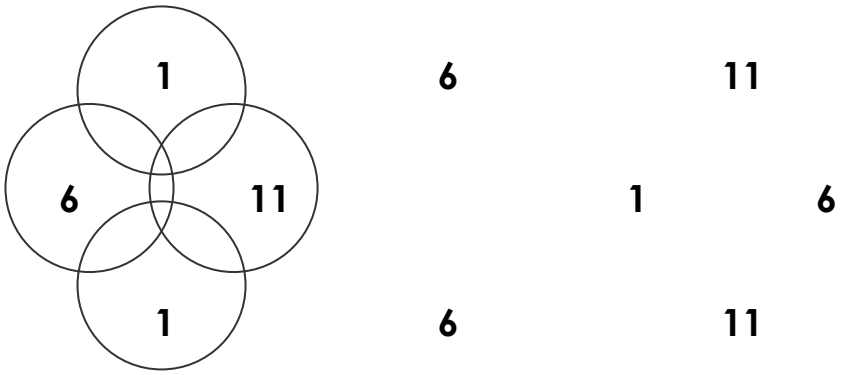


Comme la fréquence du spectre d'émission en 802.11b ou g est de 22Mhz, il faut séparer les canaux d'environ 25 Mhz pour éviter les télescopages.

Permettant donc un schéma de partage de charge classique suivant

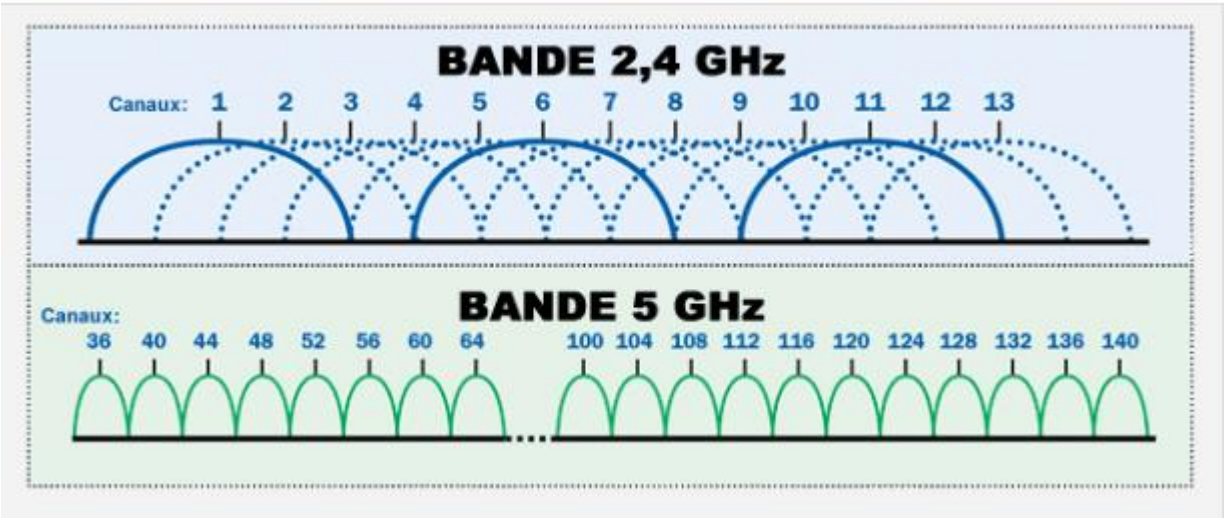


Voici un schéma de l'utilisation sur un niveau des 3 canaux classiques **1 – 6 - 11** :



Les nouveaux 802.11n – 802.11ac:

La bande (composée des 2 sous-bandes) désignée sous le nom « bande 5 GHz » et peut être utilisée par les normes Wi-Fi récentes IEEE 802.11n et IEEE 802.11ac ; la numérotation des canaux y est différente avec une numérotation « modulo 4 », Largeur des canaux est de 44Mhz (au lieu de 25 Mhz sur la bande 2,5Ghz)



802.11	Bande de fréquence	Débit théorique maximal	Portée	Congestion	Largeur canal	MIMO
n	2,4 GHz	De 72 à 288 Mbps	Bonne	Elevée	20 MHz	Non
n	5 GHz	De 72 à 600 Mbps	Correcte	Faible	20 ou 40 MHz	Oui
ac (Wave 1)	5 GHz	De 433 à 1300 Mbps	Correcte	Faible	20, 40 ou 80 MHz	Oui
ac (Wave 2)	5 GHz	De 433 à 2600 Mbps	Correcte	Faible	20, 40, 80 ou 160 MHz	Oui (+MU-MIMO)

Bande 5 Ghz - gestion des 19 canaux 802.11n-ac

N.B : Il est incompatible avec les standards **802.11a-b-g** précédant

- Débits de 540Mbps/100Mbps
- Portée de 50-60 mètres en intérieur.
- Canaux disponibles (non recouvrant) : 19
- Largeur des canaux de 20, 44M ou 160Mhz (au lieu de 25 MGhz sur la bande 205Ghz)
- Technologie **MIMO**

MIMO signifie Multiple Input Multiple Output.

Comme son nom l'indique, cette technologie permet au Wi-Fi d'exploiter simultanément plusieurs canaux. On parle par exemple de MIMO 2×2 pour deux antennes en émission et deux en réception, ce qui double le débit par rapport à une configuration sans MIMO, soit 300 Mb/s avec 40 MHz. Le

Wi-Fi N peut atteindre du MIMO 4×4, soit un maximum absolu de 600 Mb/s

Wi-Fi AC jusqu'à 8 flux en MIMO, ce qui double encore la bande passante

WEP Wired Equivalent Privacy - 802.11a - b/g

Amélioration de la sécurité en cryptant les échanges avec :

- Chiffrement **RC4**
- vecteur d'initialisation sur 24 bits
- Clé donnée au démarrage de l'échange, clé de 64 / 128 / 256 bits

Evolution WPA – WPA2 (TKIP CCMP-AES) 802.11i

WPA : Wireless Protection Access

En 2003 norme **WPA**, avec 2 variantes de sécurisation :

Un chiffrement **RC4 amélioré** est utilisé, moyennant une mise à jour, la compatibilité avec les équipements précédents est assurée.

- **WPA-PSK** (Norme SOHO): associée à **TKIP,** utilisation d'une **PSK** Pre-share key, c'est-à-dire une clé partagée,
- **WPA-Enterprise** (Norme Professionnelle) : associée à **TKIP,** utilisation d'un protocole d'authentification (de mot de passe ou de certificats) Utilisation d'un serveur **RADIUS** est préconisée

WPA 2 - 802.11i

En 2004 norme **802.11i** appelée **WPA2** avec, 2 variantes de sécurisation :

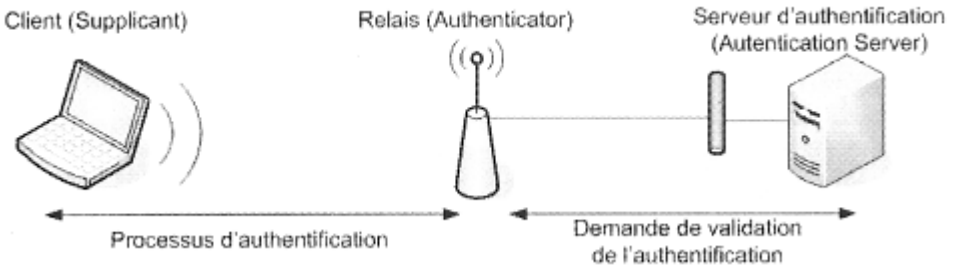
Un chiffrement **AES** est utilisé, (incompatibilité totale avec les équipements précédents. utilisant RC4)

- **WPA2-PSK** (Norme SOHO): associée à **CCMP-AES, Advanced Encryption Standard** utilisation d'une **PSK** Pre-share key, c'est-à-dire une clé partagée. (incompatibilité totale avec les équipements précédents utilisant TKIP)
- **WPA2-Enterprise** (Norme Professionnelle): associée à **CCMP-AES,** utilisation d'un protocole d'authentification selon la norme **802.1x**

Solution	Protocole	Chiffrement
WEP	WEP	RC4
WPA	TKIP	RC4+
WPA2	CCMP	AES

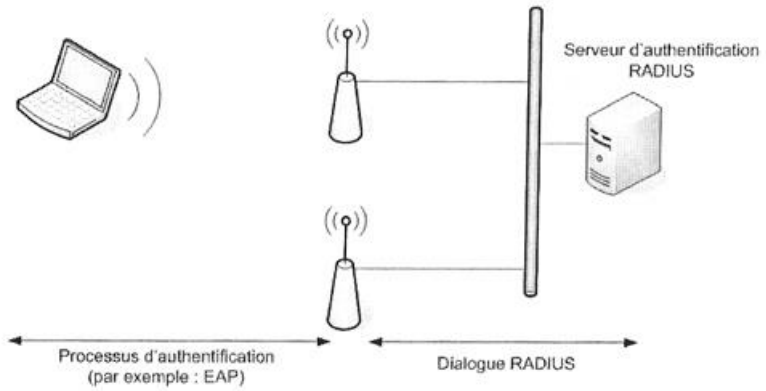
RADIUS Remote Authentification Dial In User Service

Le processus définit trois composantes



1. Le client ou système à authentifier (**Supplicant**) souhaite se connecter au réseau
2. Le point d'accès réseau , borne WI-FI (**Authenticator**) transmet la demande auprès d'un serveur d'authentification.
3. Un serveur d'authentification valide la demande (**Authentication Server**)

Le serveur préconisé par 802.11i est un serveur RADIUS



Mémo en 10 points :

1. Vérifier la compatibilité du matériel
2. Protection adresse MAC
3. changer les canaux par défaut
4. gérer voire limiter la puissance d'émission
5. si possible désactiver les différents modes et ne garder qu'une gamme de fréquence pour augmenter le débit
6. masquer le SSID
7. Eviter un serveur DHCP (ou faire de la réservation d'adresse)
8. Mettre une clé WEP minimum 128 Bits (correctement construite !), mieux si cryptage WPA WPA2
9. Placer les Points d'accès dehors du réseau interne, séparés par 1 firewall
10. Si nécessité de sécuriser, Mettre en place une authentification forte (serveur RADIUS), un VLAN, placer dessus un VPN voire de l'IPSEC

LEXIQUE WI-FI

AES :

Advanced Encryption Standard

Nouvelle technique d'encryptage utilisée en WPA2 remplaçant la technique TKIP utilisée en WPA

Adresse MAC :

Identifiant unique en hexadécimal permettant de repérer une carte réseau

Ad-Hoc :

On parle de liaison ad-hoc lorsque deux appareils équipés de carte Wifi transmettent directement entre eux, Sans passer par un point d'accès

Acces Point - Ap:

Voir point d'Accès

BSS - Basic Service Set -:

Appellation anglaise de l'architecture en mode infrastructure avec un seul Point d'Accès

DHCP :

Serveur distribuant à la demande des adresses IP préalablement déclarées. Nécessite quel client soit paramétré pour obtenir dynamiquement une adresse IP depuis le serveur DHCP, on parle alors de client DHCP.

EAP:

Extensible Authentication Protocol

C'est un mécanisme d'identification universel, fréquemment utilisé dans les réseaux sans fil et les liaisons Point-A-Point. Il est obligatoire entre les liaisons AP et client

Les standards WPA et WPA2 ont officiellement adopté plusieurs types d'EAP comme mécanismes officiels d'identification : EAP-TLS - EAP-TTLS/MSCHAPv2 - PEAPv0/EAP-MSCHAPv2 -PEAPv1/EAP-GTC -EAP-SIM

Egal à egal:

Voir Ad-Hoc

ESS - Extended Service Set:

Appellation anglaise de l'architecture en mode infrastructure étendue (plusieurs points d'Accès). On parle parfois en francais de points d'accès en mode Pont.

ESSID ou nom du réseau WIFI :

cf SSiD

IBSS - Independant Basic Service Set:

Appellation anglaise de l'architecture mode ad hoc (sans Point d'Accès)

MIMO - Multiple-Input Multiple-Output:

technologie utilisée pour les réseaux sans fil et permettant des transferts de données à plus longue portée et à plus grande vitesse que leWI-Fi

Mode Infrastructure:

On parle de mode infrastructure à partir du moment ou les appareils sont reliés entre eux via des points d'accès . Selon qu'il y ait un seul ou différents points d'accès on parlera alors de mode infrastructure (IBSS), ou de mode infrastructure en mode étendu (ESS)

Pire :

Puissance Isotrope Rayonnée Equivalente

Unité de puissance effective utilisée pour mesurer la couverture des éléments radios actif en WIFI (bornes)

PSK :

Pre-Shared Key

Clé partagée, correspondant à la présence de 2 clé identiques sur les 2 équipements qui cherchent à communiquer.

Souvent associé à **WPA** dans l'acronyme **WPA/PSK**…

Point d'Accès :

Appareil émetteur de fréquences sur lequel les clients wifi ont venir se connecter. En l'absence de point d'accès centralisateur, deux appareils équipés de Wifi peuvent transmettre directement entre eux, en un mode appellé ad-hoc.

Radius Remote Authentification Dial-In User Service

Serveur d'authentification pour les accès distants

Roaming

Action de passer de la zone de couverture d'un AP à une autre sans perdre la connexion

SSID ou ESSID ou nom du réseau WIFI :

L'**ESSID**, souvent abrégé en **SSID**, (**Service Set Identifier)**, représente le nom du réseau et est nécessaire pour qu'une station se connecte au réseau

Se paramètre sur le poste émetteur WI-FI (dit Point d'accès).

WEP

Wired Equivalent Privacy

Technique de cryptage apparue en 802.11b fondée sur une clé fixe donnée au démarrage de l'échange

Wi-Fi

Wireless fidelity

Surnom donné à la norme 802.11en 1998. Par extension s'applique a toutes les liaisons radios qui ont suivit….

WPA

Wired Equivalent Privacy

Technique de cryptage améliorée (postérieure à WEP) apparue en 2003 sur 802.11g fondée sur une clé de cryptage changée à chaque trame émise

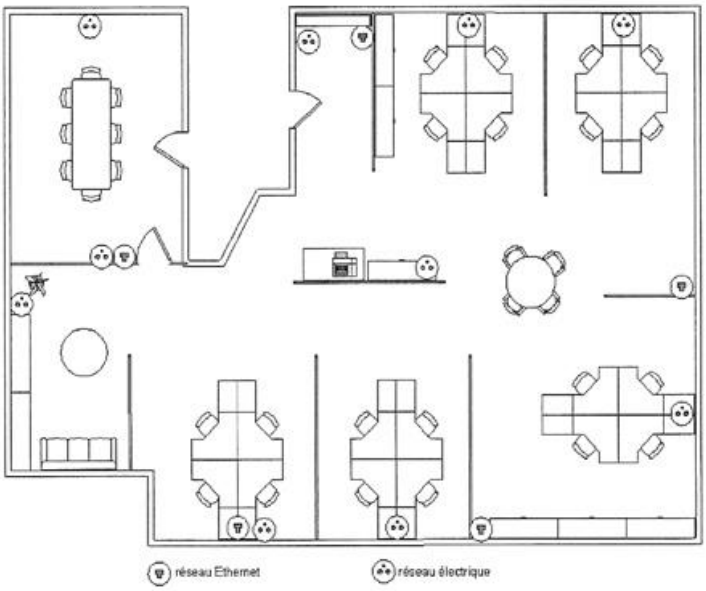
WPA 2

Evolution du WPA introduisant une Clé cryptée plus forte AES et la présence obligatoire d'un serveur d'authentification

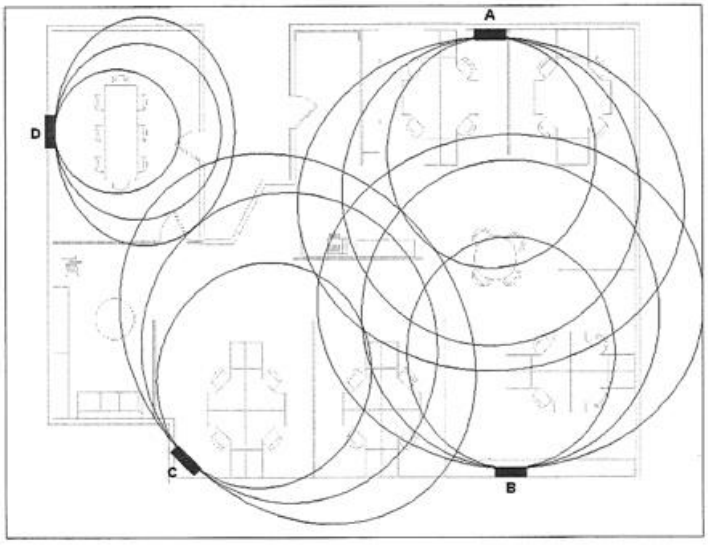
ANNEXE

cas pratique de gestion des canaux :

Soit un plan de bureaux de la sorte :



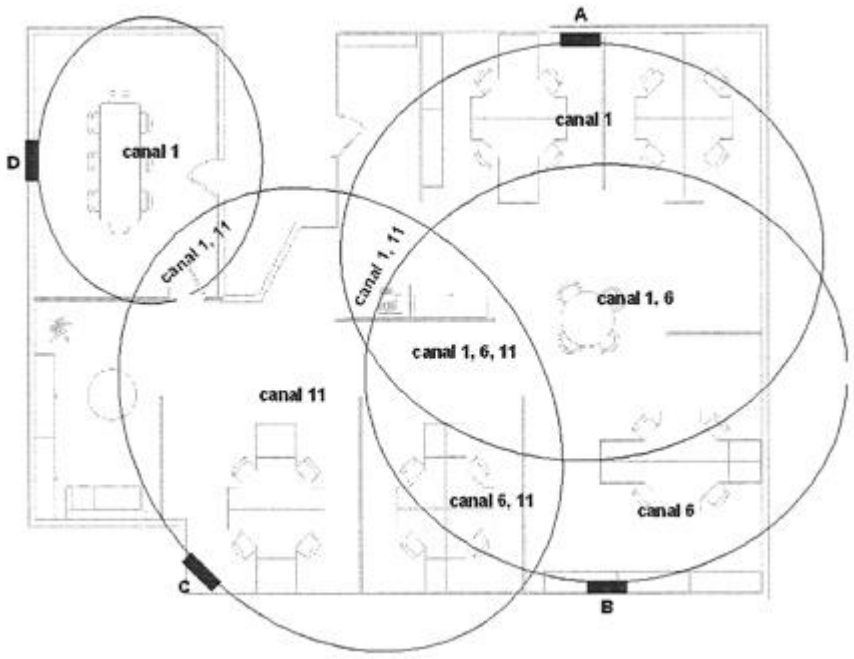
Une première approche des couvertures - puissances possibles -donnerait le schéma suivant :



Questions :

- Quels canaux choisir pour chaque Point d'accès ?
- Si le bâtiment comporte plusieurs étages "identiques", comment procéder ?

une solution pour l'étage pourrait être la suivante



S'il fallait équiper ainsi des plateaux sur plusieurs étages, comment faudrait il procéder ?

et bien pour le 1° étage, on travaille avec les fréquences

1/6/11

pour le 2° étage, avec les fréquences

2/7/12

pour le 3° étage, avec les fréquences

3/8/13