Les réseaux locaux sans fil

Dr. BEJAOUI T.

2019-2020

https://sites.google.com/site/tarekbejaoui/

Pourquoi déployer un réseau sans fil aujourd'hui ?

- Permettre la mobilité des utilisateurs
- Accès facile/rapide au réseau
- Pour faciliter la connexion des utilisateurs itinérants, en particulier dans les espaces collectifs
- Pour connecter des locaux impossibles ou trop coûteux à câbler (amiante, monument historique)
- Pour mettre en place une connexion provisoire (travaux)
- Le sans fil n'est pas destiné à remplacer intégralement le câblage filaire (fiabilité, débit)
- *Il n'est pas fait pour connecter des serveurs !*

Les technologies sans fil

Les technologies sans fil peuvent être classées en quatre parties :

- Les réseaux personnels sans fil : WPAN

- Les réseaux locaux sans fil : WLAN

- Les réseaux métropolitains sans fil : WMAN

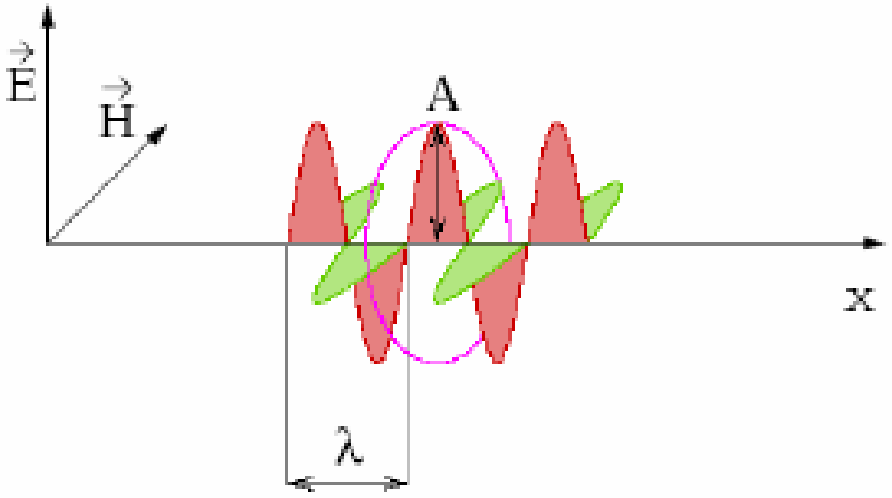
BLR (IEEE 802.16), 1 à 10 Mbps, portée 4 à 10 Km

- Les larges réseaux sans fil : WWAN

Ondes électromagnétique

Ondes radios, infra-rouge, visible, ultra-violet, X, γ…

$$\lambda \times f = c \approx 3 \times 10^{8} \, m/s \; .$$



f (GHz)	λ (cm)
0,9	33,3
1,8	16,5
2,4	12,5
5,5	5,5

Les différents types de réseaux sans fil

	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

Wi-Fi et IEEE 802.11, c’est quoi?

- Acronyme de ***w**ireless **fi**delity,* et utilisé généralement pour désigner les réseaux 802.11 de tout type, que ce soit 802.11b, 802.11a, 802.11g, 802.11n, 802.11ac, bi-bande, etc;
- Wi-Fi est une technologie sans fil qui utilise la fréquence radio pour transmettre des données à travers l’interface air:
- **IEEE 802.11** est un terme qui désigne un ensemble de normes concernant les réseaux sans fil qui ont été mises au point par le groupe de travail 11 du Comité de normalisation LAN/MAN de l'IEEE
- Le terme **802.11x** est utilisé pour désigner cet ensemble de normes et non une norme quelconque de cet ensemble comme pourrait le laisser supposer la lettre « x ».

Bref historique

- IEEE a établi le groupe 802.11 en 1990. Les spécifications pour les standards ont été ratifiées en 1997
- Les vitesses initiales étaient 1 et 2 Mbps
- IEEE a modifié le standard en 1999 pour inclure 802.11a et b
- Les équipements « 820.11b » étaient les premiers disponibles sur le marché, ensuite « a » suivi par « g ».
- 802.11g a été rajouté en 2003
- 802.11n, en 2009
- 802.11ac, en 2014
- 802.11ax, en 2019

Les standards IEEE 802.11 en Bref

802.11

	Bitrate	Spectrum	MIMO Streams	Modulation
802.11-1997	1-2 Mbps	2.4 GHz	0	DSSS, FHSS
802.11b	5.5-11 Mbps	2.4 GHz	0	DSSS
802.11a	54 Mbps	5 GHz	0	OFDM
802.11g	54 Mbps	2.4 GHz	0	OFDM
802.11n	600 Mbps	2.4-5 GHz	4	OFDM
802.11ac	1 Gbps	5 GHz	8	OFDM

Protocole	Date de normalisation	Fréquences	Taux de transfert (Typ)	Taux de transfert (Max)	Portée moyenne (intérieur) [réf. nécessaire]	Portée (extérieur) [réf. nécessaire]
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	~25 m	~75 m
802.11b	1999	2,4-2,5 GHz	6,5 Mbit/s	11 Mbit/s	~35 m	~100 m
802.11g	2003	2,4-2,5 GHz	25 Mbit/s	54 Mbit/s	~25 m	~75 m
802.11n	2009	2,4 GHz et/ou 5 GHz	200 Mbit/s	450 Mbit/s	~50 m	~125 m
802.11ac	jan. 2014	5,15-5,35 GHz 5,47-5,875 GHz	433 Mbit/s[1]	1300 Mbit/s	~20 m	~50 m
802.11ax	Est. vers fin 2020 [2]	2,4 GHz / 5 GHz		10.53 Gbit/s		

Amendement	Date de publication	Description
802.11d	2001	Permet la récupération dynamique des contraintes de transmissions (puissance max., canaux autorisés) en fonction des régulations locales.
802.11h	2003	Décrit des mécanismes permettant de mesurer et de sélectionner dynamiquement les canaux afin de respecter leurs conditions d'utilisations locales (notamment nécessaires pour l'utilisation de la bande ISM à 5 GHz en Europe[3]).
802.11i	2004	Ajoute des mécanismes d'identification et de chiffrement des données (WPA), afin de remplacer l'algorithme initial WEP de la norme 802.11 qui est obsolète.
802.11j	2004	Décrit les modifications nécessaires à l'utilisation des bandes de fréquences à 4.9 GHz et 5 GHz en conformité avec la régulation japonaise.
802.11e	2005	Ajoute des mécanismes de QoS dans les réseaux 802.11.
802.11r	2008	Vise à améliorer la mobilité entre les cellules d'un réseau Wi-Fi (le handover) et permettre à un appareil connecté de basculer plus vite d'un point d'accès vers un autre.
802.11u	2007	Elle vise à faciliter la reconnaissance et la sélection des réseaux et l'interfonctionnement avec d'autres réseaux externes tels les réseaux mobiles pour permettre l'interopérabilité entre différents fournisseurs de services.
802.11y	2008	L'intérêt de cette version tient à sa grande portée jusqu'à 5 000 m en extérieur. La fréquence utilisée est de 3.7 GHz, ce qui la rend incompatible avec les cartes "usuelles" (a/b/g/n/ac).
802.11w	2009	Augmente la sécurité des trames de management.

v · d · m

Réseaux locaux 802.11 : standards physiques [masquer]

Protocole 802.11	date[1]	Fréquence	largeur de bande	Débit binaire par flux MIMO[2]	Nombre maximum de flux MIMO	Codage / Modulation	Portée	
							Intérieur	Extérieur
		(GHz)	(MHz), (GHz)	(Mbit/s), (Gbit/s)			(mètres)	(mètres)
802.11-1997 (d'origine)	juin 1997	2,4	79 ou 22[3] MHz	1, 2 Mbit/s	NC	FHSS, DSSS	20 m	100 m
802.11a	sept 1999	5	20 MHz	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	NC	OFDM	35 m	120 m
		3,7[A]					—	5 000 m[A]
802.11b	sept 1999	2,4	22 MHz	1, 2, 5,5, 11 Mbit/s	1	DSSS	35 m	140 m
802.11g	juin 2003	2,4	20 MHz	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	1	OFDM	38 m	140 m
802.11n	oct 2009	2,4 / 5	20 MHz	7,2 à 72,2 Mbit/s[B] (6,5 à 65)[C]	4	OFDM	70 m (2,4 GHz) 12-35 m (5 GHz)	250 m[4]
			40 MHz	15 à 150 Mbit/s[B] (13,5 à 135)[C]				
802.11ac	déc 2013	5	20 MHz	6,5 à 346,8 Mbit/s	8	OFDM	12-35 m	300 m
			40 MHz	13,5 à 800 Mbit/s				
			80 MHz	19,3 à 1733,2 Mbit/s				
			160 MHz	58,5 à 3466,8 Mbit/s				
802.11ad	déc 2012	57 à 71 GHz	1,7 à 2,16 GHz	jusqu'à 6,75 Gbit/s[5]	3, 4, 6	OFDM ou simple porteuse	10 m[6]	
802.11af	février 2014	0,054 à 0,79	6 à 8 MHz	1,8 à 568,9 Mbit/s	1, 2, 4	OFDM	100 m	1000 m
802.11ah	mai 2017[1]	0,9	1 à 8 MHz	0,6 à 8 Mbit/s[7]	1, 2	OFDM	100 m	
802.11ax	2019	2,4 / 5	20 MHz	8 à 143,4 Mbit/s	8	OFDM, OFDMA	12-35 m	300 m
			40 MHz	16 à 286,8 Mbit/s				
			80 MHz	34 à 600,5 Mbit/s				
			160 MHz	68 à 1201 Mbit/s				
802.11ay	avril 2018	58,32 à 70,2	8,64 GHz	20 à 176 Gbit/s	8	OFDM, OFDMA	100 m	500

Bref historique (2)

IEEE créé les standards mais le « Wireless Ethernet Compatibility Alliance » certifie les produits.

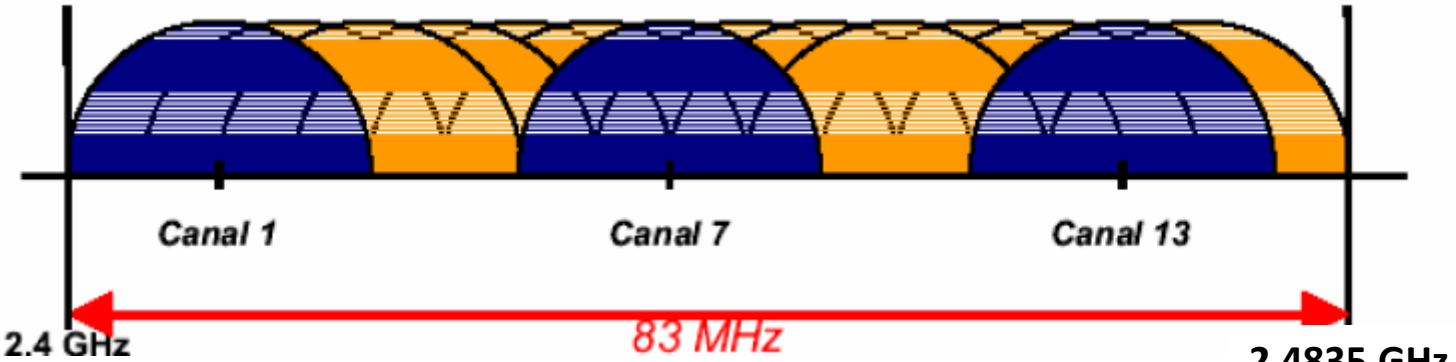
IEEE 802.11 : normalisation des WLAN

Norme d'interopérabilité du WECA

Technologie Apple

802.11b

- Fonctionne dans **la bande des 2.4 GHz** qui le rend sensible aux interférences provoquées par d'autres équipements (micro-ondes, téléphones sans fils, etc) et possède aussi des inconvénients de sécurité.
- Nombre de points d'accès intégrés limité à 3
- Possède 11/13/14 canaux (USA/Eupope/Japan), avec 3 non-recouvrant, et supporte des taux théoriques allant de 1 à 11 Mbps. En pratique autour de 4-5 Mbps max.
- Utilise la modulation de type FHSS ou DSSS (Direst-sequence spread-spectrum)



802.11b

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
11 Mbits/s	50 m	200 m
5,5 Mbits/s	75 m	300 m
2 Mbits/s	100 m	400 m

802.11g (WiFi-2)

- Extension de 802.11b, avec les mêmes inconvénients (sécurité et interférence)
- Possède une couverture radio presque similaire à celle de 802.11b
- Compatible avec 802.11b ce qui permet une transition facile du 11b au 11g
- Flexible car de multiples canaux peuvent être combinés pour une vitesse supérieure, mais limité à un seul point d'accès
- Fonctionne à 54 Mbps, mais réellement autour de 20-25 Mbps et autour de 14 Mbps lorsque « b » est associé
- Utilise la modulation OFDM (Orthogonal Frequency Division Multiplexing)

802.11g (WiFi-2)

Débit théorique	Portée (en intérieur)	Portée (à l'extérieur)
54 Mbits/s	27 m	75 m
48 Mbits/s	29 m	100 m
36 Mbits/s	30 m	120 m
24 Mbit/s	42 m	140 m
18 Mbit/s	55 m	180 m
12 Mbit/s	64 m	250 m
9 Mbit/s	75 m	350 m

802.11a (WiFi-5)

- Complètement différent de 11b et 11g
- Flexible car de multiples canaux peuvent être combinés pour une vitesse supérieure et plus de points d'accès peuvent coexister
- Couverture inférieure à celle de 11b et 11g
- Fonctionne dans ***la bande des 5 GHz***, donc moins d'interférences que les autres équipements
- Possède 12 canaux, 8 non-recouvrant et supporte des taux allant de 6 à 54 Mbps, mais réellement autour de 27 Mbps max
- Utilise la modulation OFDM (Orthogonal Frequency Division Multiplexing)

802.11a (WiFi-5)

Débit théorique (en intérieur)	Portée
54 Mbits/s	10 m
48 Mbits/s	17 m
36 Mbits/s	25 m
24 Mbits/s	30 m
12 Mbits/s	50 m

802.11b+

- Non standard, fonctionne dans la bande des 2.4 GHz
- Compatible avec le 802.11b
- Supporte des débits théoriques allant de 1 à 22 Mbps. En pratique, autour de 6 Mbps max
- Utilise une technique de modulation complètement différente.

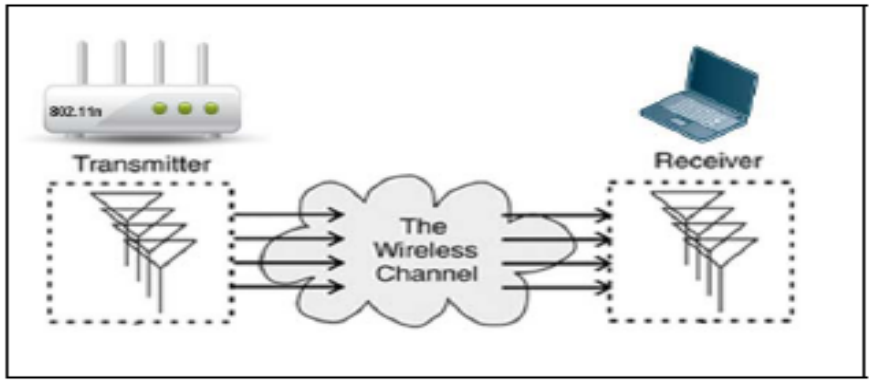
802.11n

- Doit permettre d'atteindre un débit théorique pouvant atteindre 300 Mbits/s;
- Fonctionne dans la bande de fréquences des 2.4 GHz ou 5 GHz;
- Apporte des améliorations par rapport à IEEE 802.11a/b/g grâce aux technologies suivantes:
  - MIMO qui permet d'utiliser, à la fois, plusieurs émissions spatiales et plusieurs antennes d'émission et de réception
  - Le regroupement des canaux radio permettant d'augmenter la bande passante
  - L'agrégation de paquets de données qui permet l'augmentation des débits

802.11n : Le MIMO

- Actuellement, en 802.11a/b/g, la communication entre les mobiles et les points d'accès utilise une seule émission spatiale et une seule antenne;
- Le MIMO introduit la possibilité d'utiliser deux (ou plus) émissions spatiales et de recevoir les signaux sur plusieurs antennes;
- Le signal d'origine est recomposé en utilisant des techniques de multiplexage radio avancées;

802.11n : Le MIMO (2)



- On parle de MIMO 2x3 (300Mbps) ou 3x3 (450 Mbps) ou 4x4 (600 Mbps)
- L'état actuel des composants électroniques du marché ne permettant pas de dépasser les 2x3 sur les produits pour l'entreprise, nous sommes au 300 Mbps → permet donc d'envoyer 2 fois plus de données (2x72 Mbps=144Mbps) grâce à ses 2 émetteurs

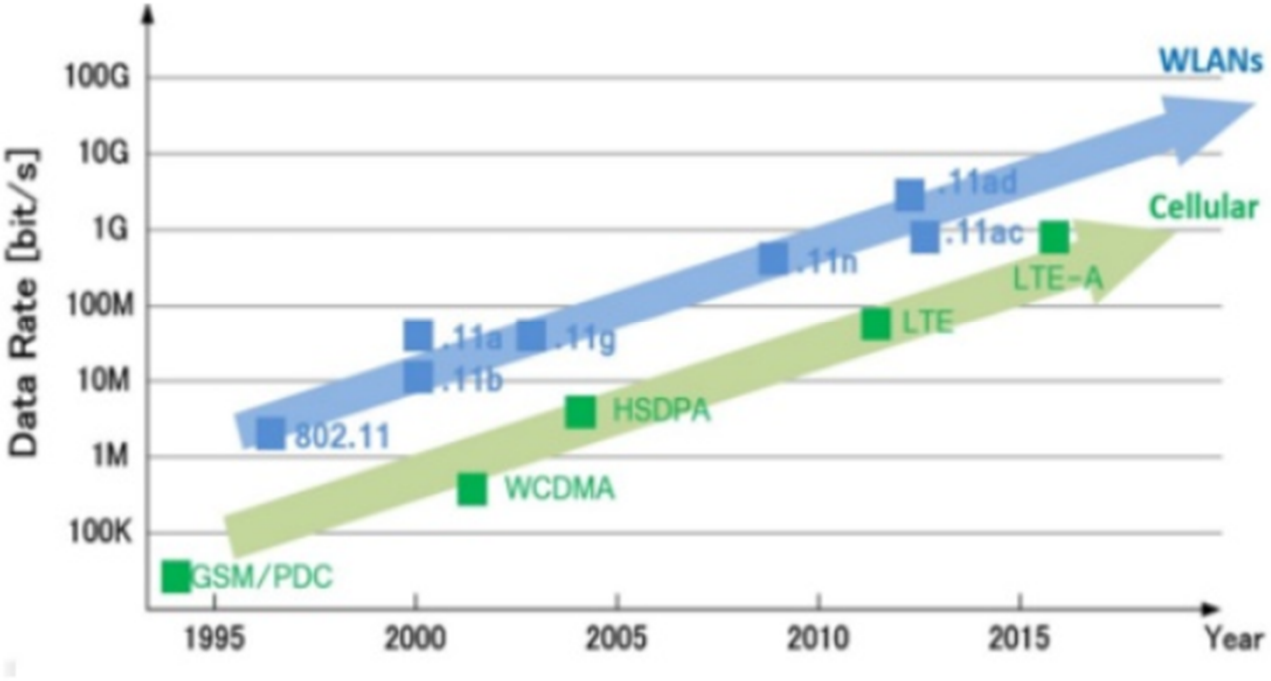
802.11n : Regroupement des canaux radio

- Lors d'une émission radio, l'un des moyens conventionnels permettant d'augmenter la BP est d'augmenter la largeur du canal d'émission radio;
- 802.11a/b/g utilise des canaux d'une largeur de 20 MHz;
- Le 802.11n permet le regroupement de 2 canaux traditionnels pour réaliser un canal d'émission de 40 mHz;
- L'agrégation des canaux permet de passer de 144 Mbps à 300 Mbps

802.11n : Agrégation des paquets

- Le mécanisme du 802.11 a introduit des entêtes et des silences dans l'émission radio, nécessaire pour la synchronisation;
- Afin de diminuer la proportion de ces temps de silence par rapport à l'émission de plus en plus rapide des données, le 802.11n introduit l'agrégation des paquets dans une même trame d'émission radio;
- Cette technique permet d'augmenter le ratio débit utile/débit théorique en n'utilisant qu'un seul entête radio pour plusieurs paquets de données

Du plus Haut Débit



802.11ac

- Publiée en 2013
- Une largeur de canal de 80 MHz, pouvant aller jusqu'à 160 MHz. En 802.11n, le maximum était de 40 MHz.
- Utilisation de différents flux spatiaux en MIMO
- Support de 8 flux spatiaux au maximum, contre 4 en 802.11n, dont 4 flux downlink multi-utilisateurs (MU-MIMO)
- Modulation Haute densité en QAM à 256 états, contre 64 états en 802.11n
- Certaines implémentations non standardisées proposent une
- modulation QAM à 1024 états, soit un débit 25% plus élevé.
- Beamforming standardisé. En comparaison, le beamforming en 802.11n ne permettait pas une compatibilité entre les équipements de fournisseurs différents

802.11ax

- Le groupe 802.11ax a été crée en 2013

L'objectif est :

  - Amélioration des performances du WLAN et supporter les transmissions multi-utilisateurs
  - Utilisation efficace des ressources spectrales
  - Amélioration des performances en scénarios denses
  - Amélioration de l'efficacité énergétique
  - Fournir une rétrocompatibilité

- Standard finalisé au courant de 2020

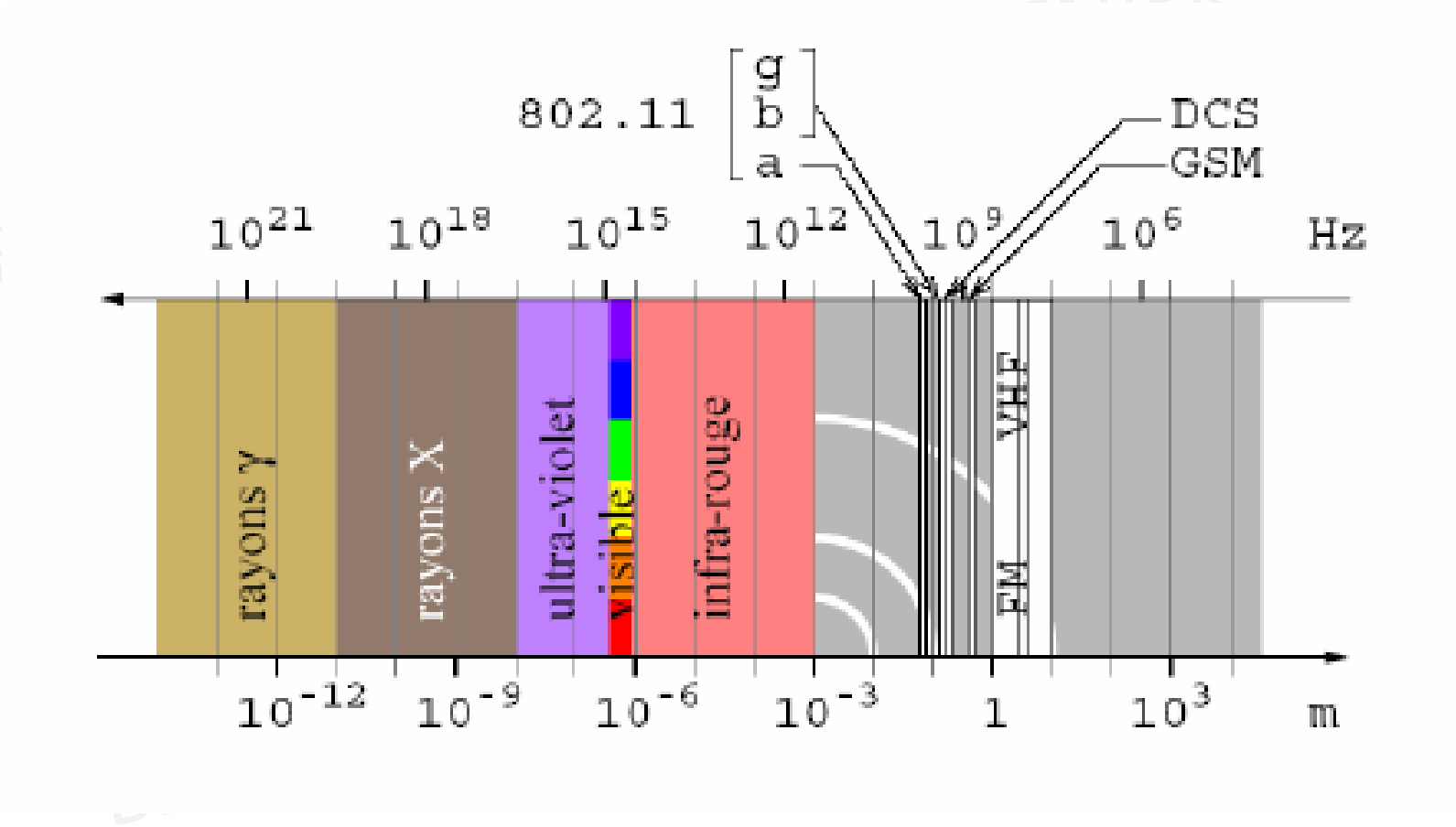
Autres normes 802.11

- 802.11f (2003) : Inter Access Point Protocol (IAPP) gestion de la mobilité
- 802.11h (2003) : pour l'utilisation de 802.11a en Europe sélection dynamique de canal et gestion de la puissance d'émission
- 802.11i (2004) : sécurité
- 802.11e (2005) : qualité de service
- 802.11k : mesure de la qualité de la liaison radio
- 802.11n : débit > 100 Mb/s
- 802.11r : transfert rapide de connexion entre bornes
- 802.11s : réseaux maillés

ISM

- Industrial/Scientific/Medical bands
- 902-928 MHz
  - Crowded: Cordless phone, wireless speaker, garage door (telemetry)
- 2400-2483.5 MHz
  - Medium use, Microwave oven
- 5725-5850 MHz
  - US & Canada only
  - Light use, some radar
  - Expensive

Spectre électromagnétique



Rôle de l'AP

- Gestion radio
- Gestion du protocole 802.11 (couche MAC, les trames…)
- Gestion de la connexion au réseau filaire grâce à un pont Ethernet/802.11 et d'une pile de protocole IP permettant d'embarquer le logiciel de configuration.
- Gestion de l'administration et de la sécurité de réseau

Les différents modes de fonctionnement des AP

- Fonction « racine »
- Fonction « Pont » ou « Brigde »
- Fonction « client »
- Fonction « répéteur »

Interfaces disponibles sur un point d'accès WiFi

- RJ45 : utilisé généralement pour interconnecter le réseau à un autre réseau (filaire…) ou un terminal ne disposant pas de carte Wi-Fi
- RJ11 : sert pour les accès ADSL
- RJ14 : utilisé pour l'accès console (administration)
- Port USB : pour connecter d'autres périphériques en USB

Caractéristiques d'un terminal WiFi

Pour qu'un poste soit connecté à un réseau Wi-Fi il est indispensable qu'il soit équipé de l'un des éléments suivants :

- Carte PCMCIA Wi-Fi généralement utilisé pour les PC Portable
- Carte PCI Wi-Fi pour les PC ou autres
- Une clé USB Wi-Fi pour tout périphérique équipé d'un port USB



- Un adaptateur Wi-Fi quelconque : Ethernet/Wi-Fi ou Port parallèle/Wi-Fi ou Port série/Wi-Fi


Architecture

1. Architecture cellulaire

- Similaire à la téléphonie mobile : téléphones + stations
- Un ou plusieurs points d'accès : unifier le réseau et servir de pont

2. Topologies

Il existe deux types de topologies :

- mode infra-structure

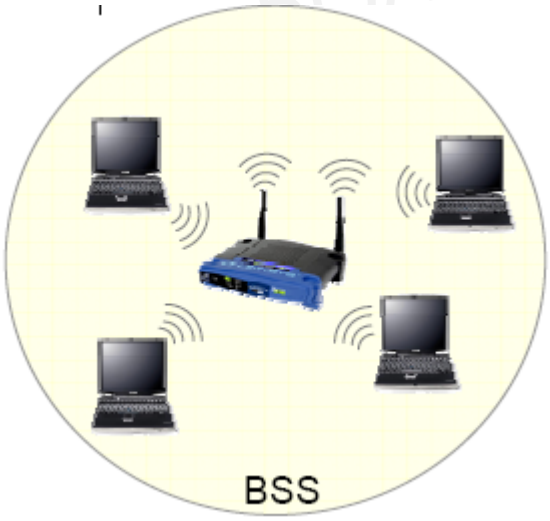
- BSS : Basic Service Set
- ESS : Extended Service Set

- mode ad-hoc

- IBSS Independent Basic Services Set

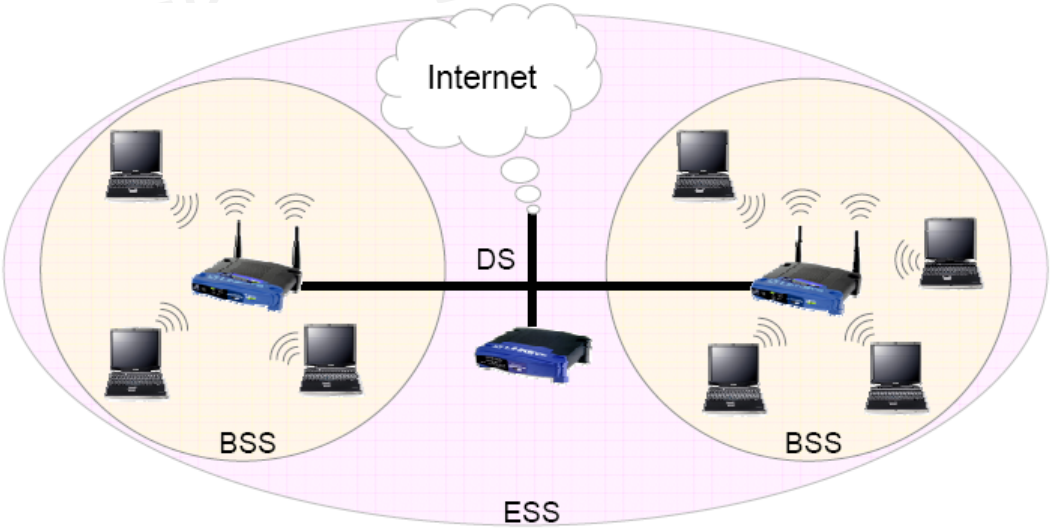
Le mode infrastructure : BSS

- Le mode infratsructure désigne un réseau composé d'une infrastructure permettant l'échange d'information entre les stations ; l'infrastructure est le point d'accès
- 1 cellule = 1 Basic Service Set (BSS) = 1 point d'accès
- N stations : support partagé entre toutes les stations, ainsi que le débit



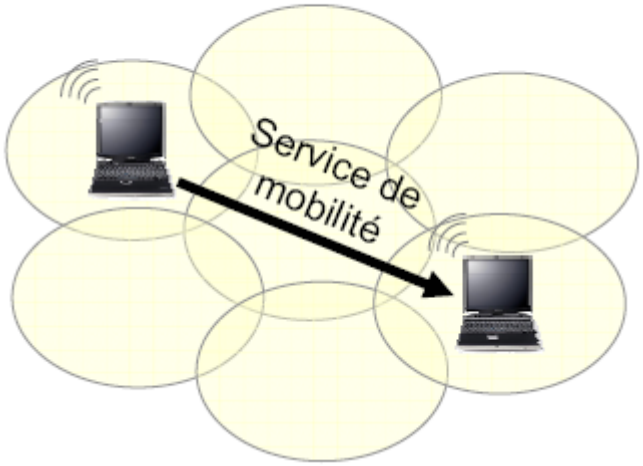
Le mode infrastructure : ESS

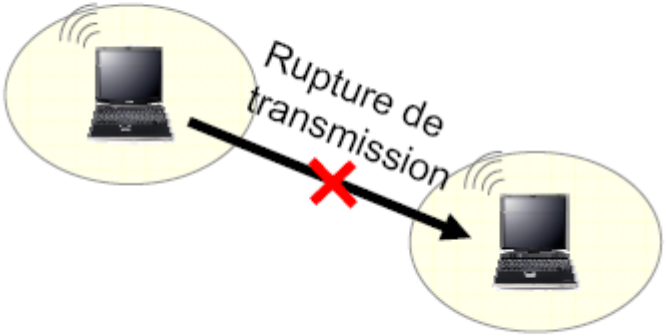
- Plusieurs points d'accès (BSS) connectés entre eux par un système de distribution (DS)
- Le DS peut être un réseaux Ethernet ou un autre réseau WLAN
- Elle permet la fourniture d'accès vers un autre réseau : Internet



Le mode infrastructure : ESS

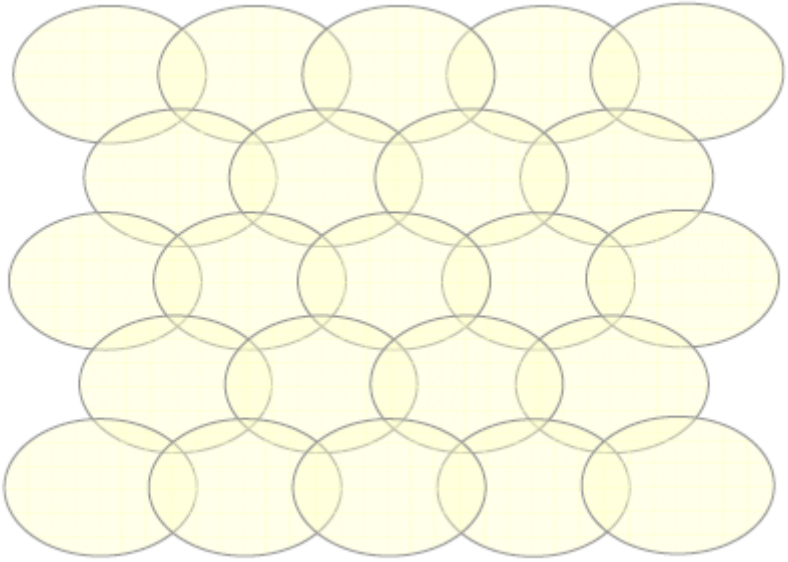
- La topologie ESS peut être variable : cellules recouvrantes ou non.
- Les cellules recouvrantes permettent d'offrir le service de mobilité (IEEE 802.11f) : pas de pertes de connexions
- Plus grand nombre d'utilisateurs possibles sans dégradations trop importantes des performances.





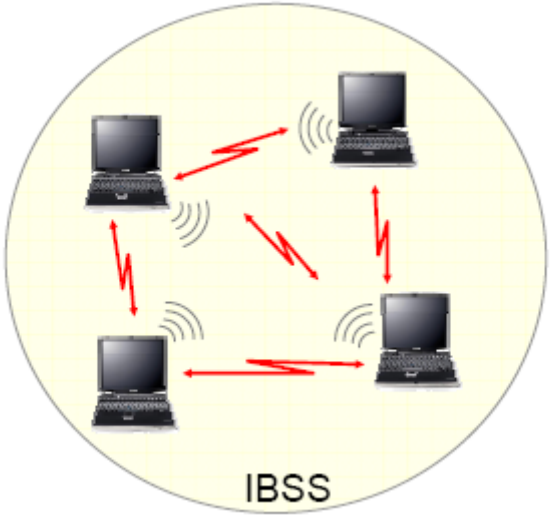
Réseau ambiant

- Le mode ESS permet d'obtenir un réseau ambiant
- permet de se connecter à Internet de partout
- constitué de nombreuses cellules qui possèdent chacune un point d'accès
- les points d'accès sont reliés entre eux par un réseau d'infrastructure (Ethernet, GigE, IEEE 802.17, etc)



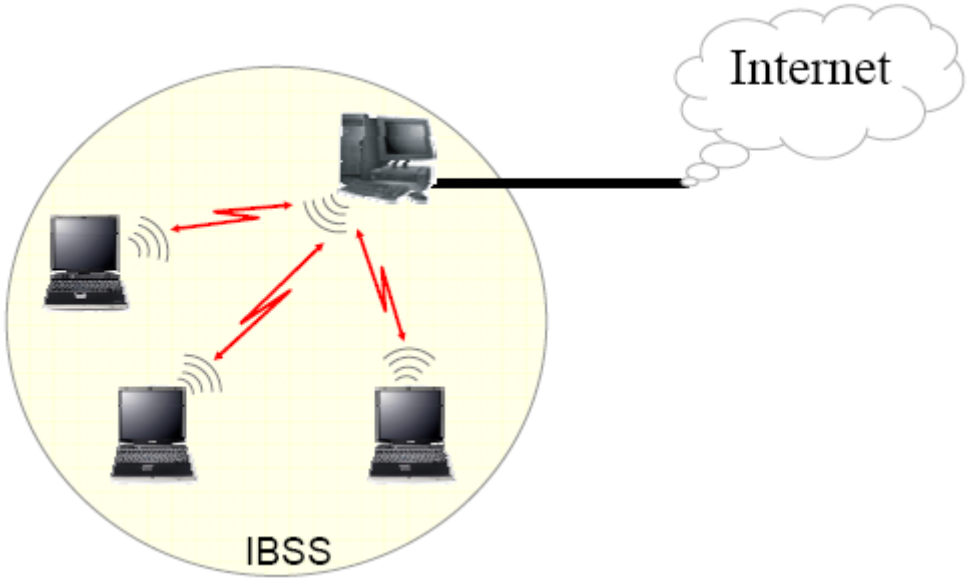
Le mode Ad hoc : IBSS

- Independent Basic Service set: c'est le mode point à point. Il permet l'échange d'informations lorsqu'aucun point d'accès n'est pas disponible



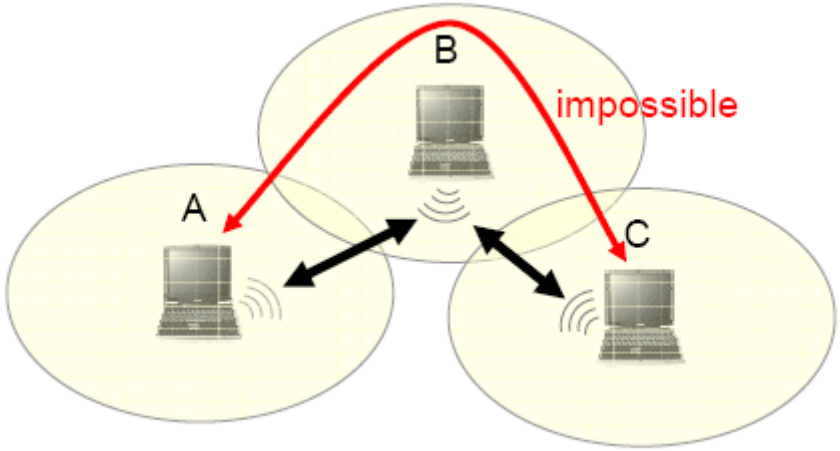
Le mode Ad hoc

- En mode Ad hoc, une station peut partager un accès à Internet : le réseau fonctionne comme un BSS.



Le mode Ad hoc

- un réseau à 3 stations en mode ad hoc est différent d'un réseau ad hoc de 3 stations
- il n'ya pas de protocole de routage : A ne peut pas envoyer de données à C car B ne peut pas effectuer le routage.



3 stations en mode ad-hoc

Réseaux Ad-hoc et routage

- L'algorithme de routage doit être implémenté au niveau de chaque nœud
- Solution la plus simple : routage directe : toutes les stations peuvent se voir sans passer par un nœud intermédiaire
- Cas le plus classique : nœuds intermédiaires dotés de tables de routages optimisées
- Problèmes pour la construction des tables :
  - Liaisons asymétriques
  - Interférences
- Normalisation des réseaux ad-hoc :
  - Protocoles réactifs
  - Protocoles proactifs

Protocoles réactifs

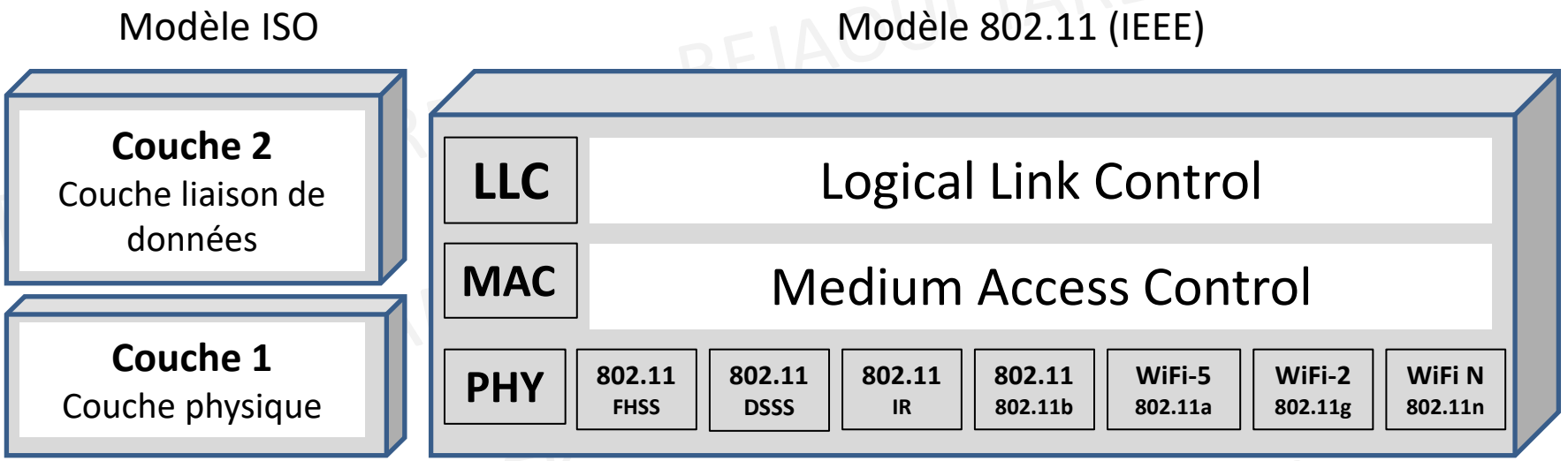
- Travaillent par inondation : détermination de la meilleure route lorsque les paquets sont prêts à être émis
- Pas d'échange de paquets de contrôle sauf paquets de supervision (détermination du chemin)
- Le paquet de supervision diffusé vers les nœuds voisins est transmis par ceux-ci vers le nœud de destination : plusieurs routes possibles si problèmes sur la route principale

Protocoles proactifs

- Emission ininterrompu de paquets de supervision
- Maintien de la table de routage : rafraîchissement dynamique
- Chaque information de supervision influençant le comportement du réseau entraîne la modification des tables
- Difficulté : calcul des tables de routage pour qu'elles soient cohérentes

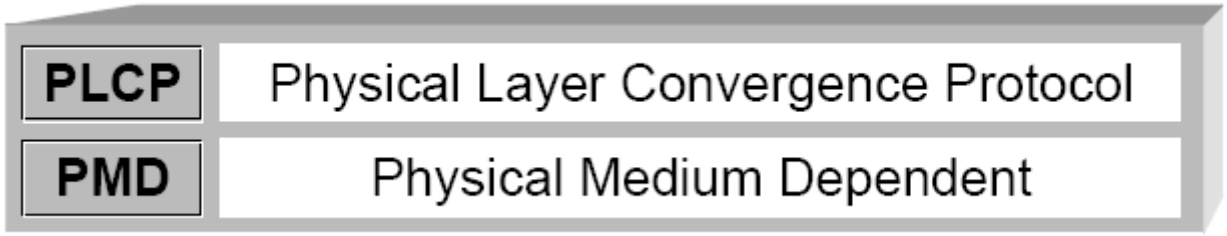
Architecture des systèmes
IEEE 802.11x

Architecture en couches



- Modèle IEEE : couche liaison de données subdivisée en deux sous-couche MAC et LLC
- Couche MAC commune à toutes les couches physiques

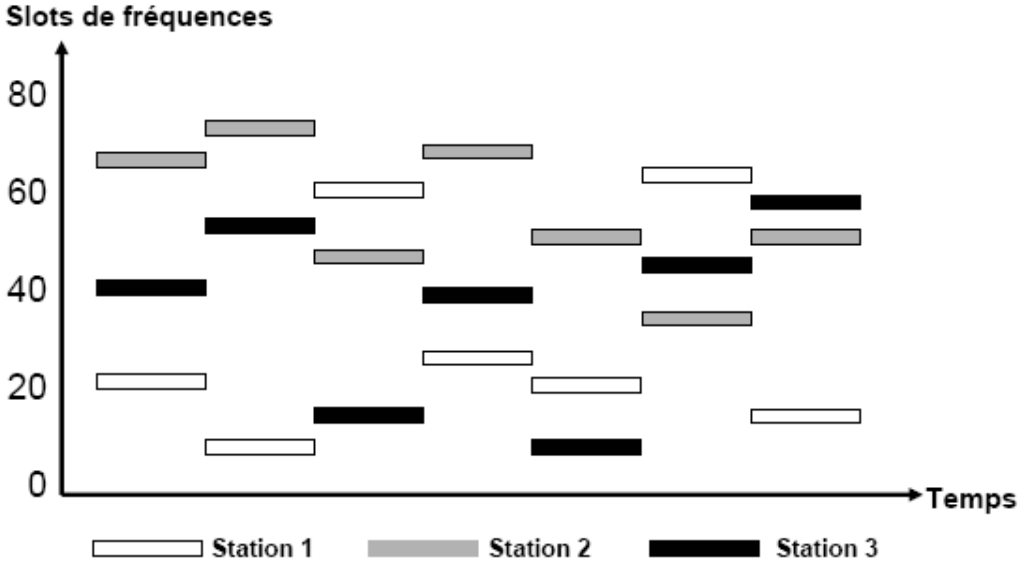
La couche physique : PHY



- Composée de 2 sous-couches :
  - PMD gère l'encodage des données et de la modulation
  - PLCP gère l'écoute du support et signale à la couche MAC que le support est libre par un CCA (Clear Channel Assessment)

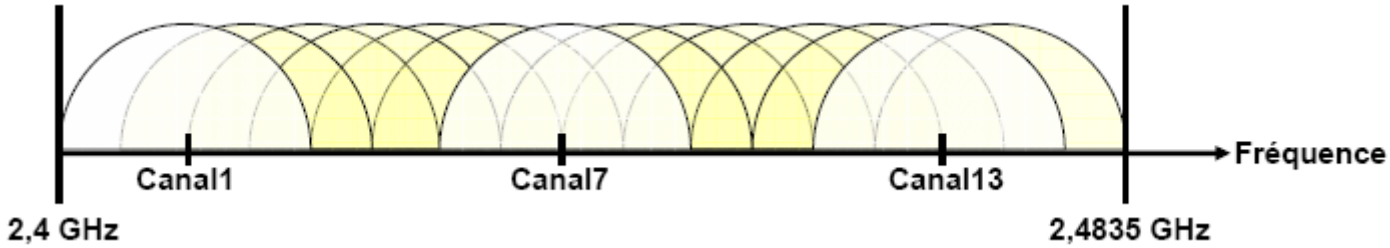
Frequency Hopping Spread Spectrum (FHSS)

- Principe : la commutation rapide entre plusieurs canaux de fréquence, utilisant un ordre pseudo aléatoire connu tant à l'émetteur qu'au récepteur pour la synchronisation.
- Les équipements radio participant à une transmission utilisant FHSS doivent utiliser la même séquence de saut de fréquence pour pouvoir communiquer.
- Bande divisée en 79 canaux (23 en France) de 1 MHz de largeur de bande
- 3 ensembles de 26 séquences, soit 78 séquences de sauts possibles
- Exemple : 3 stations sur 7 intervalles de temps : émission simultanée mais pas sur le même canal

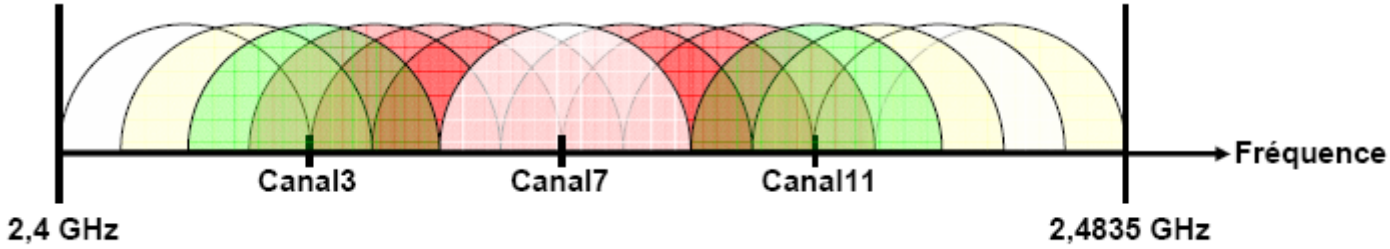


Direct Sequence Spread Spectrum (DSSS)

- Technique utilisée pour le 802.11b
- 14 canaux de 20 MHz
- Fréquences de crête espacées de 5 MHz
  - Canal 1 = 2,412 GHz; canal 14 = 2,477 GHz

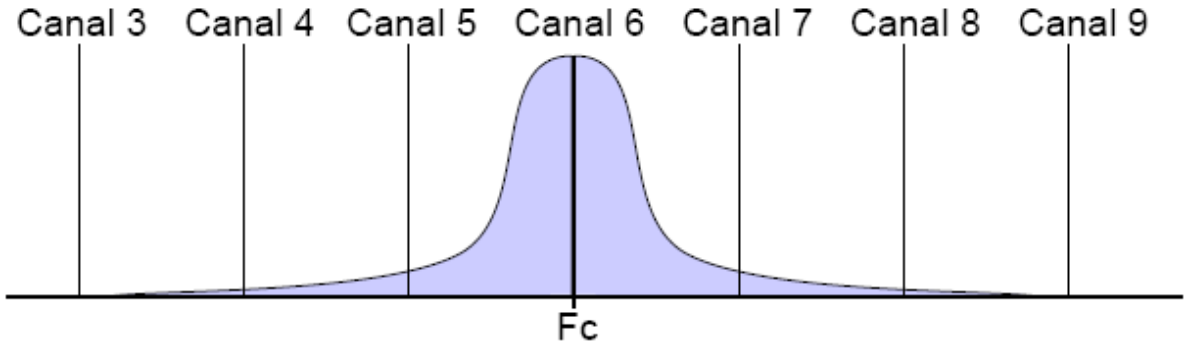


- Largeur totale de la bande = 83,5 MHz
- Canaux recouvrant : inexploitables simultanément



Direct Sequence Spread Spectrum (DSSS)

- Un seul canal utilisé par transmission : sensible aux interférences
- Plusieurs réseaux co-localisés doivent utiliser des canaux espacés de 25 à 30 MHz pour ne pas interférer



Spectre d'un canal

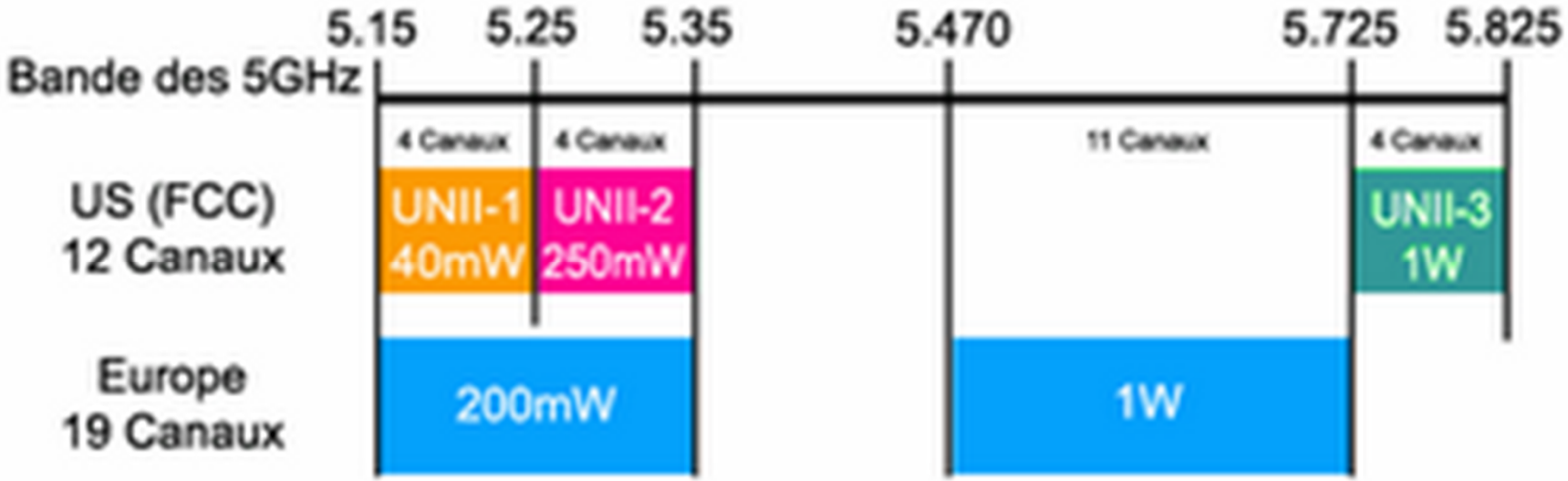
- La bande passante utilisée par un canal s'étale sur les canaux voisins

Orthogonal Frequency Division Multiplexing (OFDM)

- bande U-NII (5 GHz)

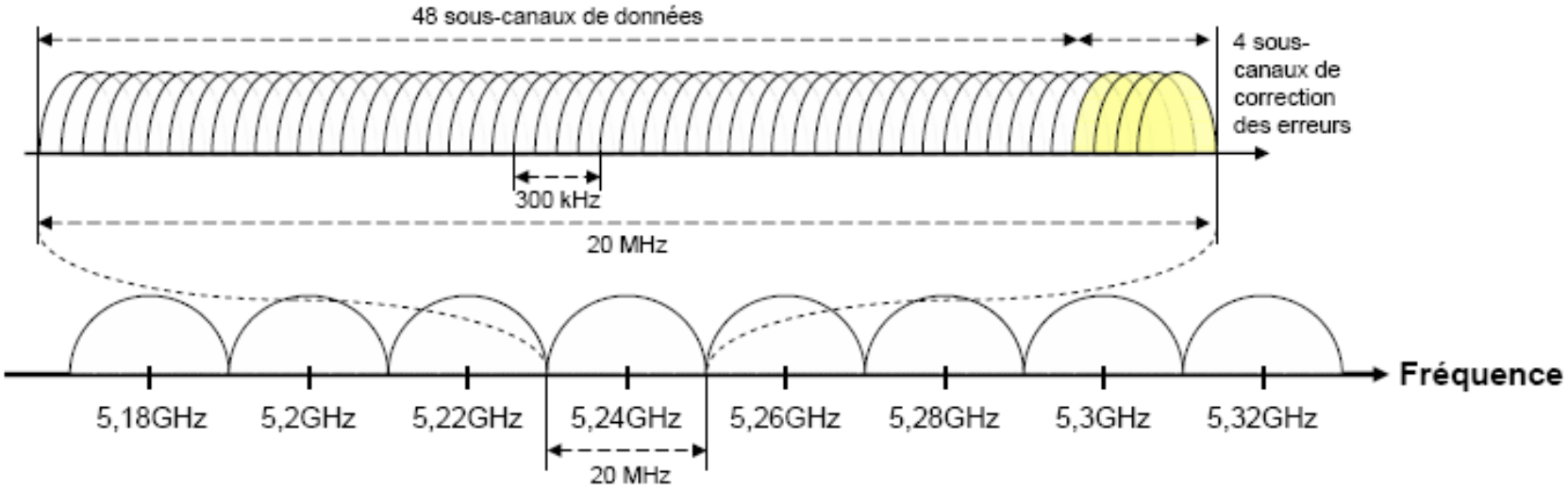
• La bande U-NII (5 .15-5.35 GHz, 5.725-5.825 GHz) offre une bande passante totale de 300MHz, chacune utilisant une puissance de signal différente.

• Division des 2 premières sous-bandes en 8 canaux de 20 MHz



Orthogonal Frequency Division Multiplexing (OFDM)

- chaque canal contient 52 sous-canaux de 300 kHz
- utilisation de tous les sous-canaux en parallèle pour la transmission
- débit de 6 à 54 Mbits/s :
  - modulation BPSK : 0,125 Mbits/s par sous-canal : total 6 Mbits/s
  - modulation QAM64 : 1,125 Mbits/s par sous-canal : total 54 Mbits/s



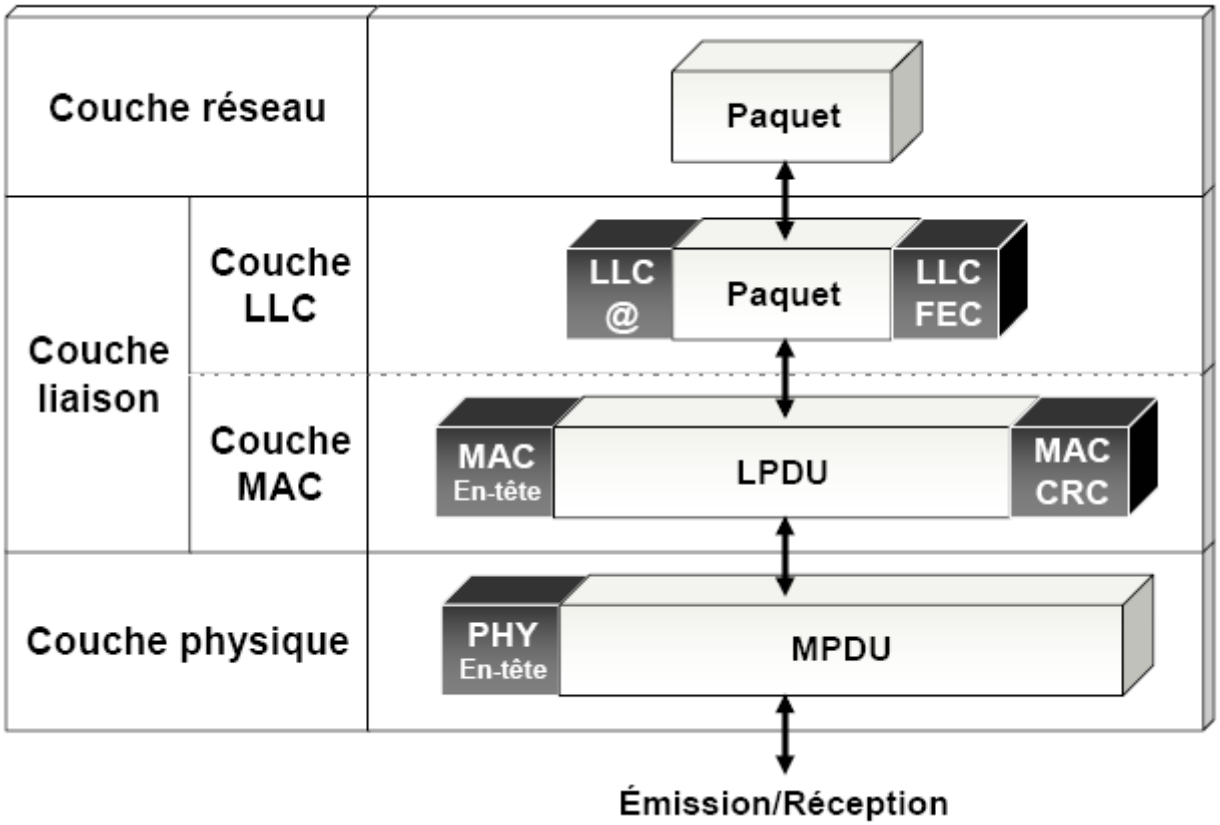
La couche Liaison de données

- La couche LLC
  - définie par le standard IEEE 802.2
  - lien logique entre la couche MAC et la couche réseau (OSI 3)
    via le LSAP : *Logical Service Access Point*
  - deux types de fonctionnalités :
    - système de contrôle de flux
    - système de reprise sur erreur
  - Le LSAP permet de rendre interopérables des réseaux différents aux niveaux MAC ou physique, mais possédant la même LLC
  - LDPU : *Logical Protocol Data Unit*

    - DSAP : *Destination Service Access Point*
    - SSAP : *Source Service Access Point*
    - Contrôle : type de LLC (avec/sans connexion avec/sans acquittement)

La couche Liaison de données

- La couche LLC



La couche Liaison de données

- La couche MAC
  - similaire à la couche MAC d'Ethernet (IEEE 802.3)
  - fonctionnalités :
    - contrôle d'accès au support
    - adressage et formatage des trames
    - contrôle d'erreur par CRC
    - fragmentation et réassemblage
    - qualité de service
    - gestion de l'énergie
    - gestion de la mobilité
    - sécurité
  - deux méthodes d'accès :
    - DCF (*Distributed Coordination Function*) : avec contention ; support de données asynchrones ; chances égales d'accès au support ; collisions
    - PCF (*Point Coordination Function*) : sans contention ; pas de collisions ; transmission de données isochrones (applications temps-réel, voix, vidéo)

Distributed Coordination Function

DCF

- méthode d'accès générale pour le transfert de données asynchrones, sans gestion de priorité
- repose sur le CSMA/CA

Le CSMA/CA

Carrier Sense Multiple Access / Collision Avoidance

- accès aléatoire avec écoute de la porteuse : évite plusieurs transmissions simultanées, réduit le nombre de collisions
- impossible de détecter les collisions : il faut les éviter
  - écoute du support
  - back-off
  - réservation
  - trames d'acquittement positif

Distributed Coordination Function

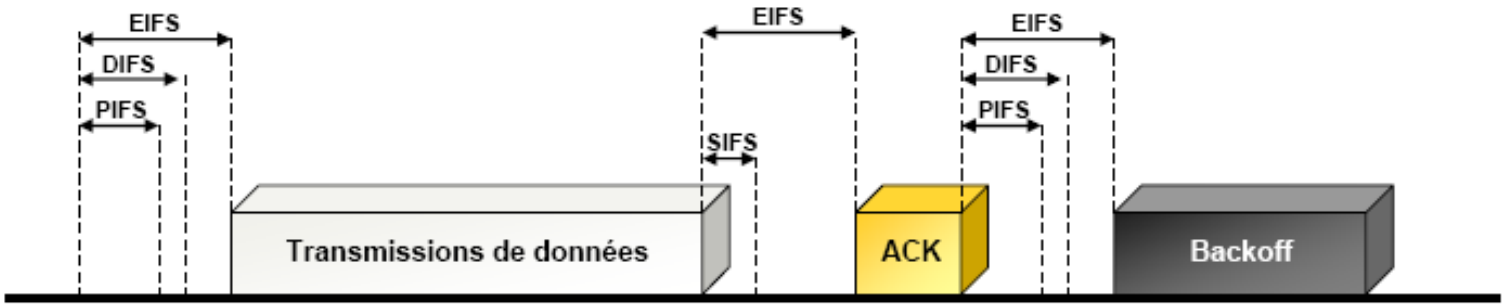
- Le CSMA/CA consiste donc à déterminer l'activité du canal par son écoute
- L'activité du canal est déduite par la détection d'une onde porteuse effectuée au niveau physique mais également par une onde porteuse virtuelle faite au niveau de la couche MAC
- Au niveau physique, la présence d'une onde est due à l'émission d'un nœud
- Au niveau logique, la porteuse est déduite de la durée de la transmission en cours qui a été annoncée dans l'en-tête de la trame
- Les nœuds à la réception de cette information l'enregistrent dans leur vecteur d'allocation réseau (NAV: Network Allocation Vector)
- La durée de la transmission comprend un temps inter-trame et le temps de transmission d'un ACK

Distributed Coordination Function

- L'écoute du support
  - Couche PHY : *Physical Carrier Sense* (PCS)
    - détecte et analyse les trames
    - fait appel au PLCP (Physical Layer Convergence Protocol)
  - Couche MAC : *Virtual Carrier Sense* (VCS)
    - réserve le support via le PCS
    - deux types de mécanismes :
      - réservation par trames RTS/CTS (Request To Send / Clear To Send)
      - utilisation d'un timer (NAV : Network Allocation Vector) calculé par toutes les stations à l'écoute
    - utilisation optionnelle : trames RTS/CTS à 1 Mbits/s, font chuter le débit moyen de 11 Mbits/s à 6 Mbits/s

Distributed Coordination Function

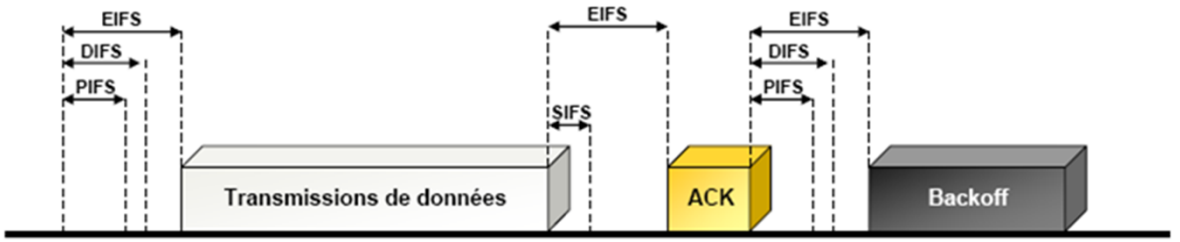
- L'accès au support
  - mécanisme d'espacement entre deux trames : IFS
  - 4 types d'*Inter-Frame Spacing* :
    - **SIFS : *Short IFS* :** sépare les différentes trames d'un même dialogue (données et ACK, RTS et CTS, différents fragments d'une trame segmentée, trame de polling en mode PCF)
    - **PIFS : PCF IFS** = SIFS + 1 timeslot : accès prioritaire, mode PCF
    - **DIFS : DCF IFS** = SIFS + 2 timeslots : mode DCF
    - **EIFS : Extended IFS :** le plus long, uniquement en mode DCF, lorsqu'une trame de donnée est erronée attente de l'acquittement



Distributed Coordination Function: procédure (1)

L'accès au support

- Une station ayant un paquet à transmettre écoute le canal
- elle doit vérifier que le canal est resté inoccupé pendant une période au moins égale à un délai appelé DIFS
- Si le canal est occupé ou devient occupé, le nœud doit retarder sa transmission jusqu'à ce que le support redevienne libre pendant une durée de DIFS
- Si le canal est libre durant une période de temps égale à DIFS, la station transmet
- Sinon, si le canal est occupé (immédiatement après ou durant le DIFS), la station continu à contrôler le canal jusqu'à ce qu'il est recensé libre durant un DIFS
- À ce moment, la station génère un intervalle de *backoff* aléatoire avant transmission (ceci est la caractéristique permettant d'éviter la collision du protocole), pour minimiser la probabilité de collision avec des paquets ayant été transmis par d'autres stations



Distributed Coordination Function: procédure (2)

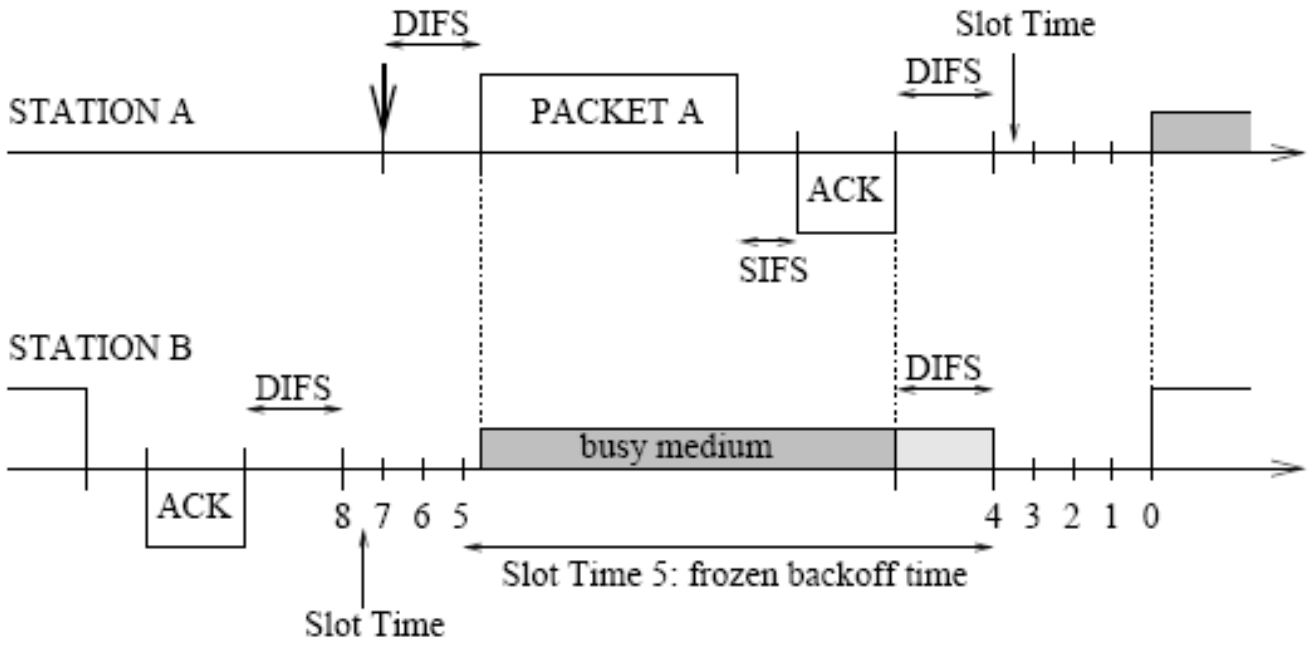
- Ce retard est déterminé par le tirage d'une valeur aléatoire appelé le délai de *backoff*
- Le backoff suit une loi exponentielle
- Pour des raisons d'efficacité, DCF emplois une échelle de backoff à temps discret
- À chaque transmission de paquet, le temps de *backoff* est uniformément choisit dans l'intervalle [0,CW-1].
- CW est appelé fenêtre de contention et dépend du nombre de transmission de paquets échouées
- À la première tentative de transmission, CW est égale à CW_{min}
- La taille de cette fenêtre est fonction du nombre de tentatives de transmission
- Après chaque transmission infructueuse, CW est doublée jusqu'à une valeur maximale $CW_{max}=2^m Cw_{min}$

Distributed Coordination Function: procédure (3)

- Une station doit attendre un temps de backoff aléatoire entre deux transmissions consécutives de nouveaux paquets, même si le canal est récencé idle durant le DIFS
- Le compteur de temps de backoff est décrémenté tant que le canal est à l'état inoccupé, et « gelé » lorsqu'une transmission est détectée sur le canal, et réactivée lorsque le canal redevient à l'état inoccupé encore une fois pour une durée supérieure à DIFS
- Le temps suivant immédiatement un idle DIFS est slotté, et une station est permise à transmettre au début de chaque Slot Time.
- La taille σ du Slot time, est le temps nécessaire à chaque station pour détecter la transmission d'un paquet par tout autre station
- σ dépend du niveau physique
- La station transmet lorsque le temps de backoff atteint 0

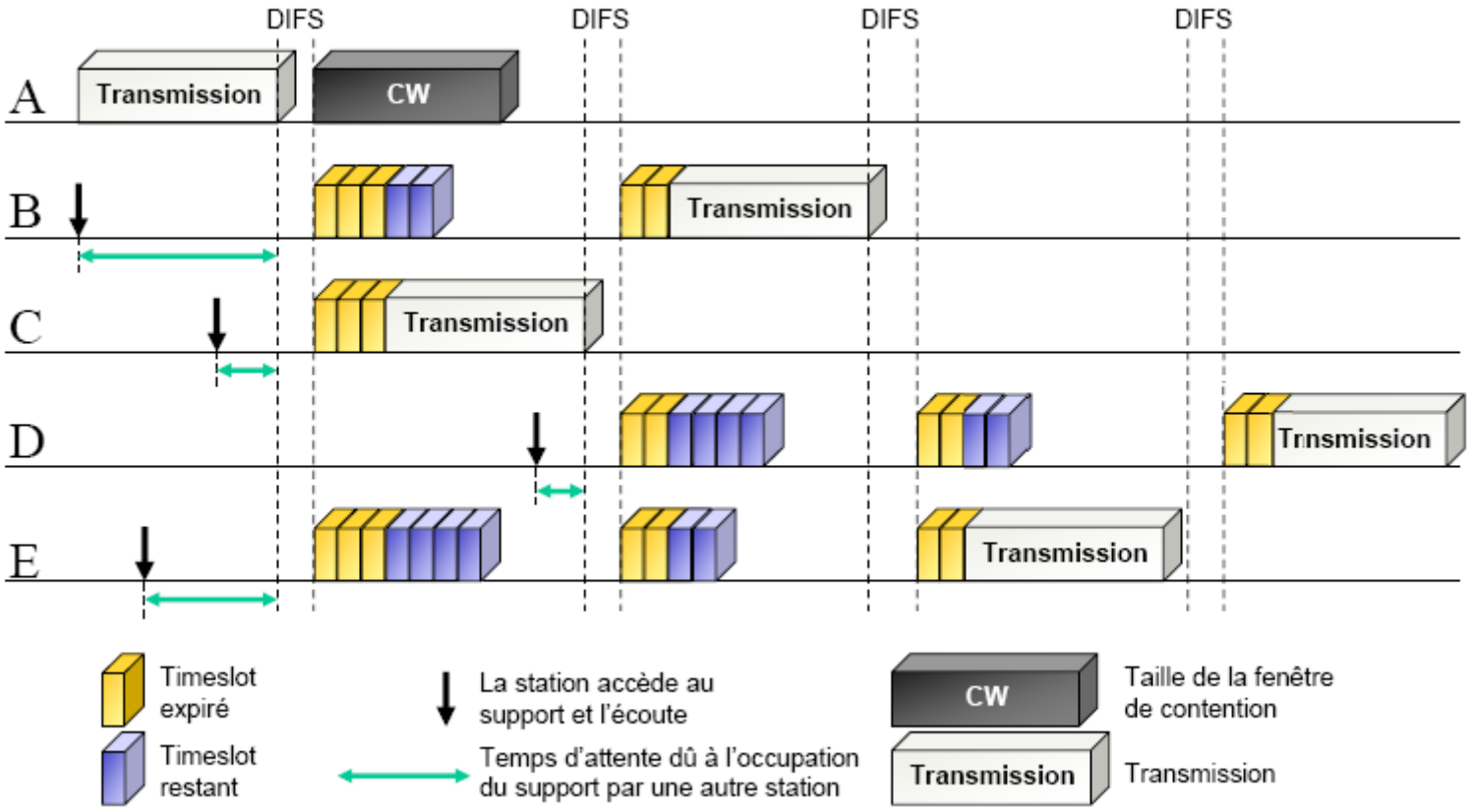
PHY	Slot Time (σ)	$CW_{\min}$	$CW_{\max}$
FHSS	50 μs	16	1024
DSSS	20 μs	32	1024
IR	8 μs	64	1024

Distributed Coordination Function



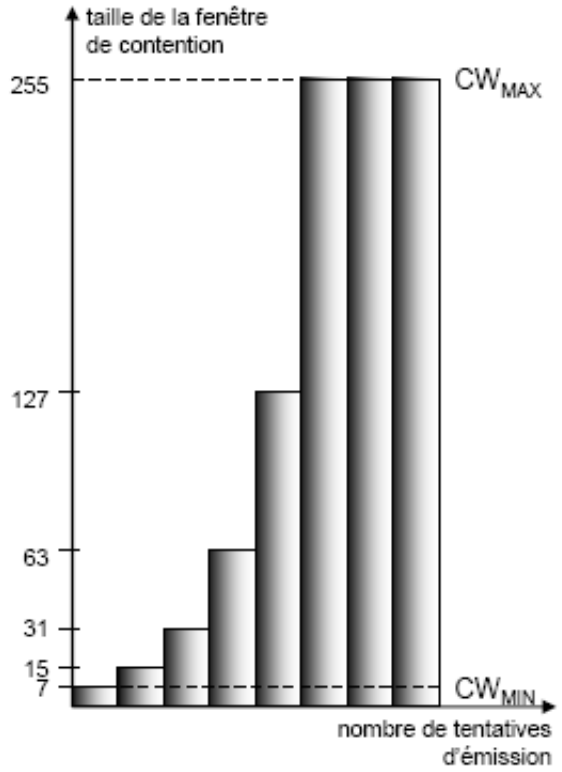
Distributed Coordination Function

- Le *back-off*
  - fenêtre de contention CW, et un *timer* $T_{backoff}$=random(0,CW)×timeslot



Distributed Coordination Function

- La contention
  - ❖ en cas de collision la fenêtre de contention CW est doublée



- ❖ le tirage au sort de la durée d'attente s'effectue sur un intervalle plus grand
- ❖ deux stations qui sont entrées en collision ont une probabilité plus faible mais non nulle d'entrer à nouveau en collision
- ❖ $n^{ième}$ tentative de transmission :

$$T_{backoff}(i) = random(0, CW_i) \times timeslot$$

$$CW_i = 2^{k+i} - 1$$

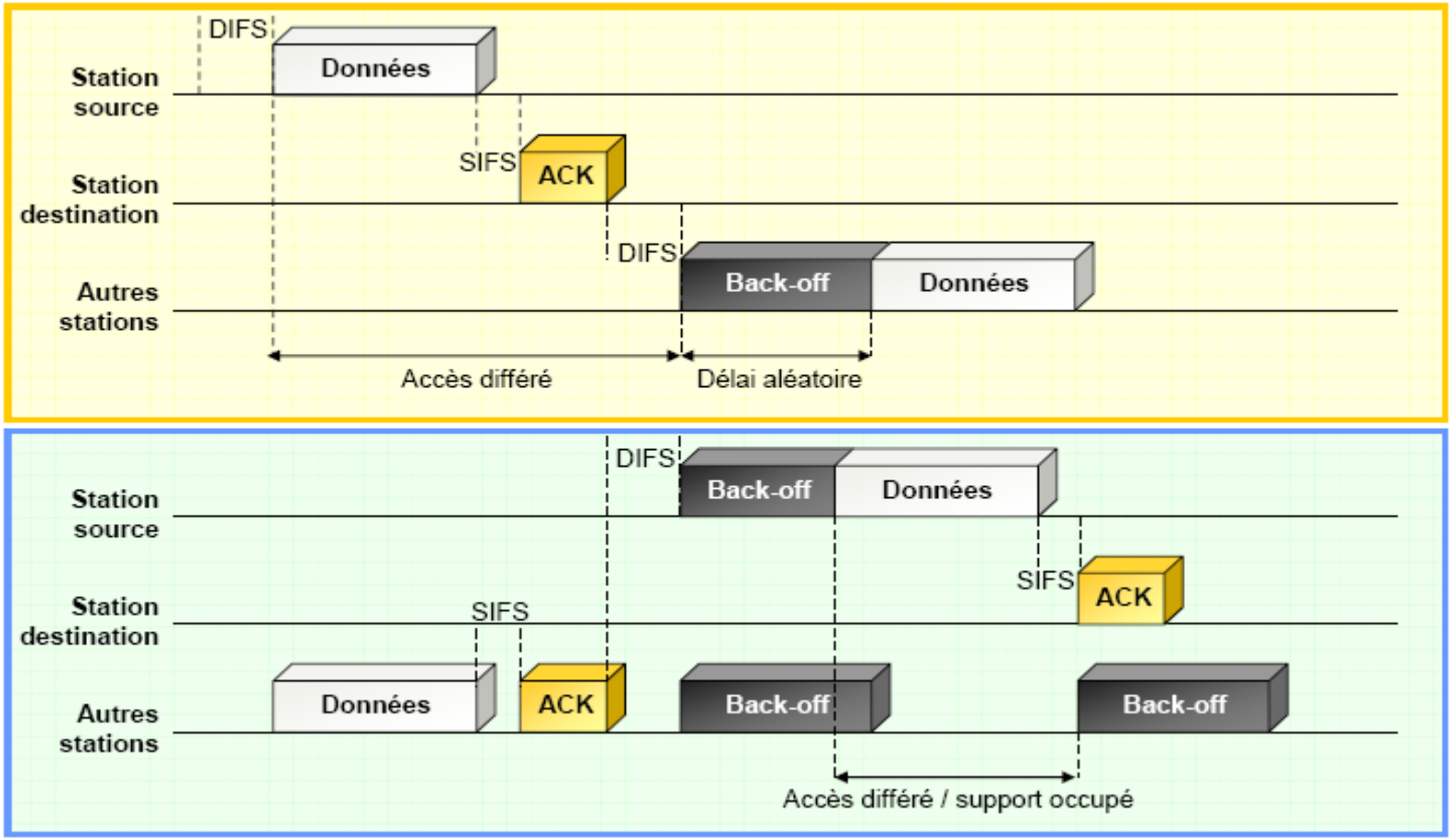
❖ chaque tentative infructueuse de transmission indique que l'étalement des demandes dans le temps n'a pas été assez important. Le tirage doit se faire sur un intervalle plus important.

Distributed Coordination Function

- La contention
  - ❖ une fois la trame émise et le délai SIFS (Short Inter Frame Space) écoulé, l'émetteur doit recevoir un ACK. Autrement, la trame de données émise est considérée comme perdue, le nombre de tentative est incrémenté et la procédure de backoff est reprise

Distributed Coordination Function

- Exemples de transmissions

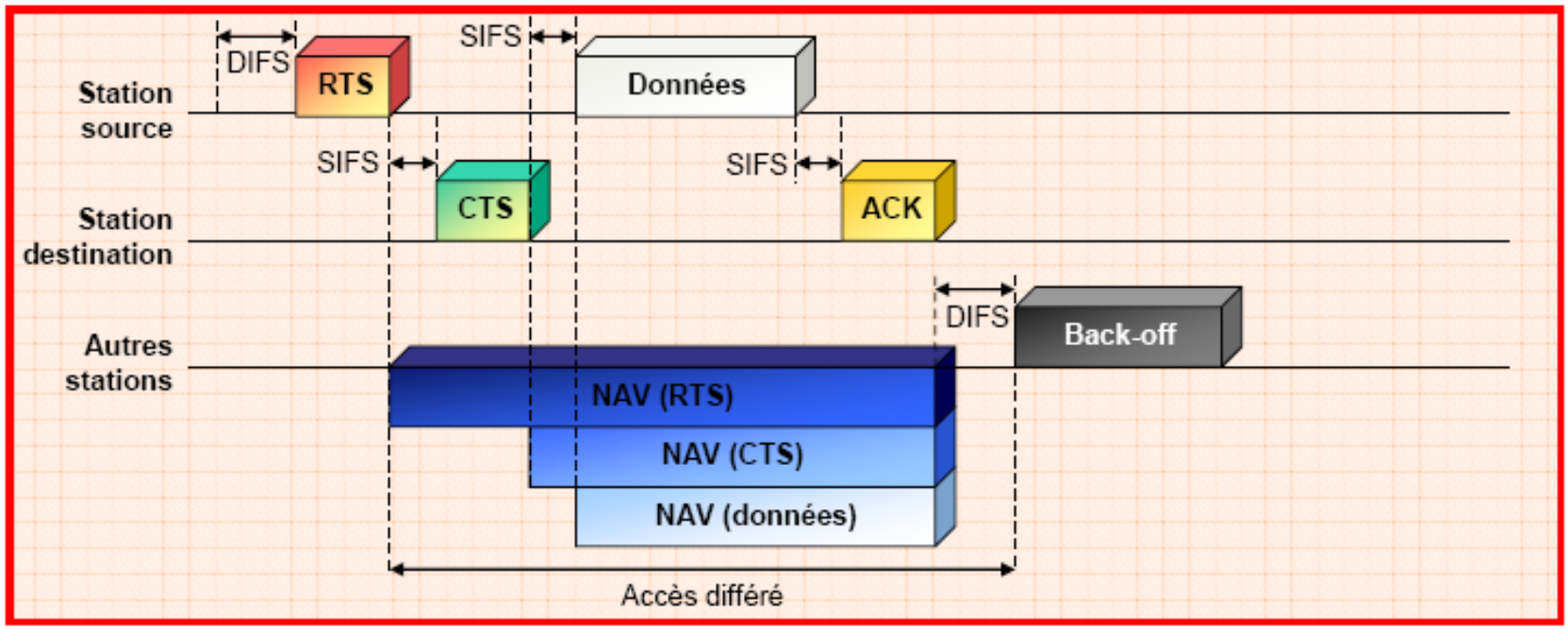


Distributed Coordination Function

- DCF prend en compte l'atténuation du signal par l'introduction du délai EIFS (Extended Inter-Frame Space)
- Quand un nœud reçoit une trame dont il peut décoder au niveau MAC, il se met en retrait pour une période EIFS afin de ne pas interférer dans la transmission en cours
- La période EIFS est environ 7 fois plus longue que la période DIFS

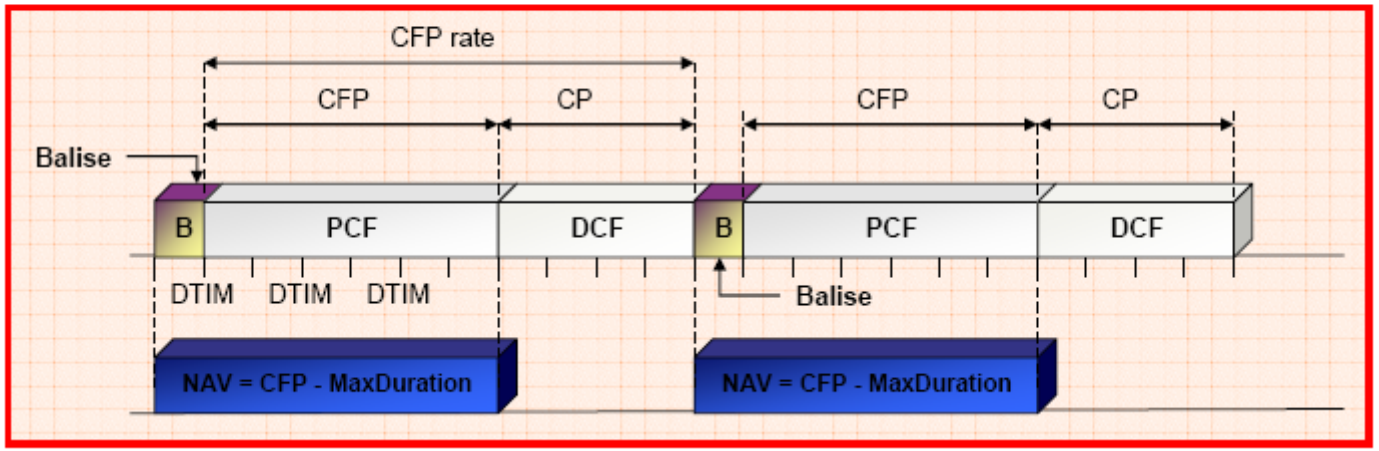
Distributed Coordination Function

- Exemples de transmissions avec réservation



Point Coordination Function

- PCF (Jamais utilisée car non implantée par les fabricants)
  - transfert temps-réel (voix, vidéo), services de priorité
  - l'AP (*Access Point* : point d'accès) prend le contrôle du support et choisit les stations qui peuvent transmettre : *polling*
- Contention
  - l'AP définit un PC (Point Coordination) avec 2 périodes :
    - CP (*Contention Period*) : période de temps avec contention et DCF
    - CFP (*Contention Free Period*) : période de temps sans contention et PCF



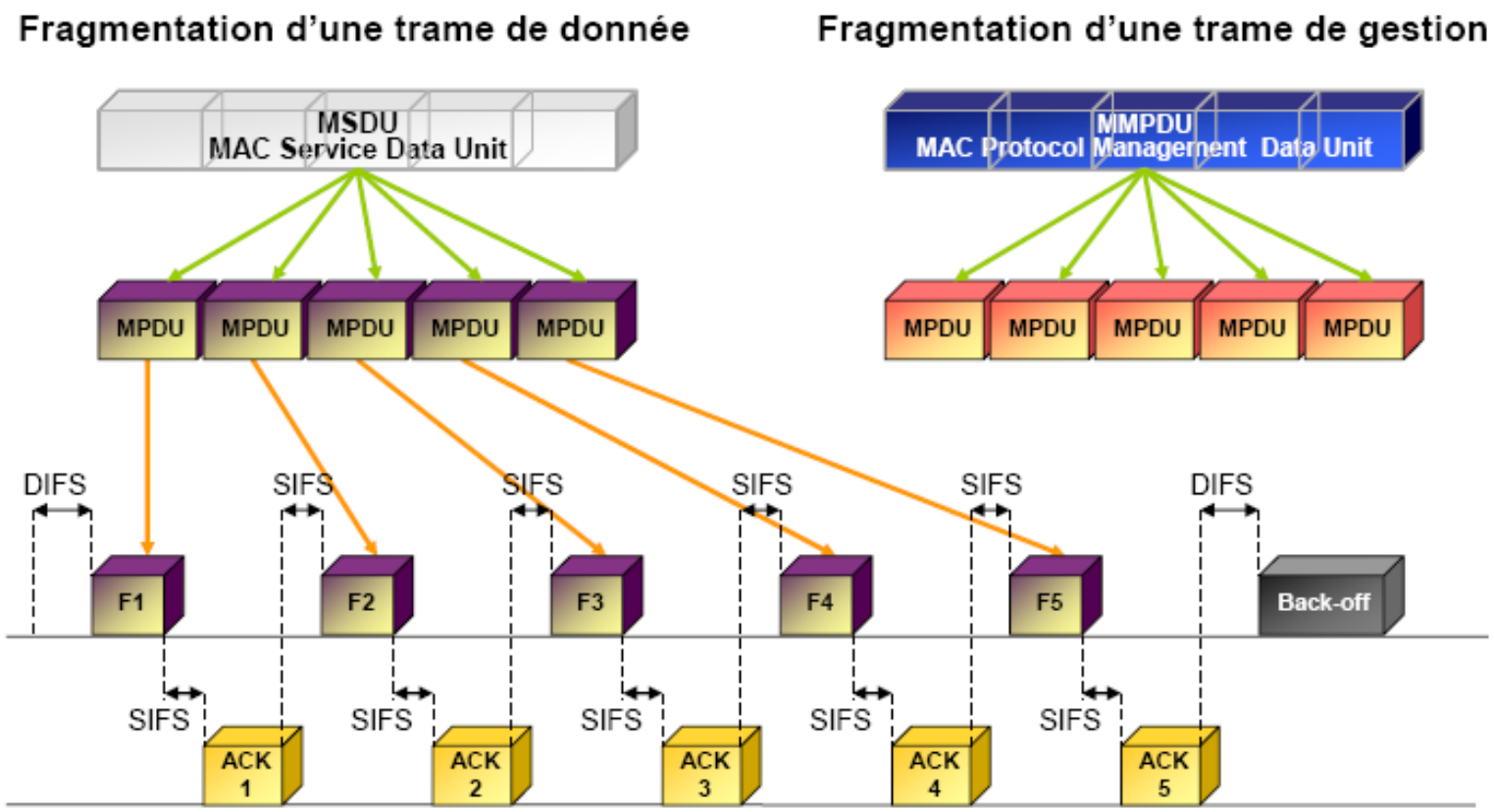
Fonctionnalités

Fragmentation et réassemblage (1)

- Taux d'erreur pour liaison sans fil très supérieur à celui des liaisons filaires : nécessité de transmettre de petits paquets
- Fragmentation d'une :
  - trame de donnée MSDU (*MAC Service Data Unit*)
  - trame de gestion MMPDU (*MAC Management Protocol Data Unit*)
  - en plusieurs trames MPDU (*MAC Protocol Data Unit*)
- Fragmentation si taille > valeur seuil
  - fragments envoyés de manière séquentielle
  - destination acquitte de chaque fragment
  - support libéré après transmission de tous les fragments
- Utilisation du RTS/CTS
  - Seul le premier fragment utilise les trames RTS/CTS
  - Le NAV doit être maintenu à jour lors à chaque nouveau fragment

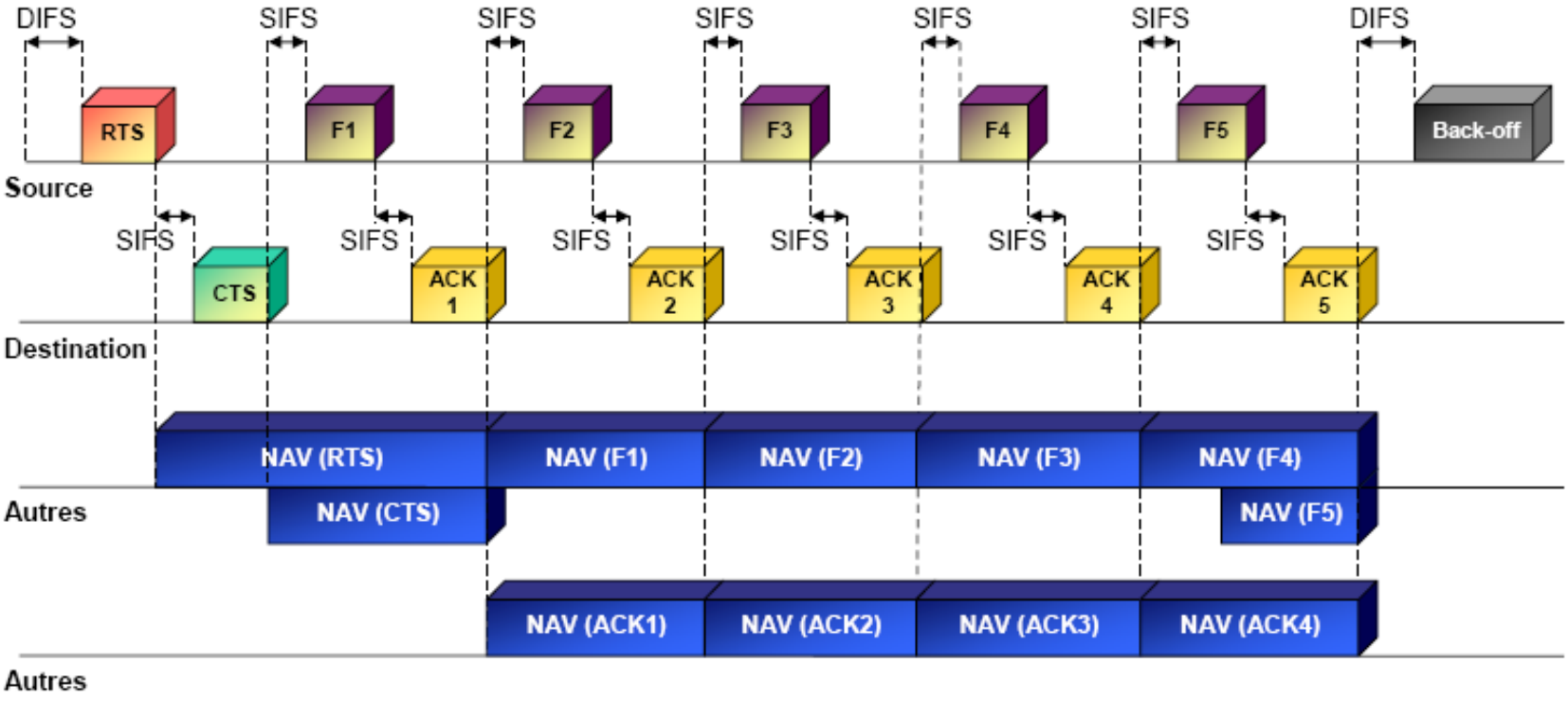
Fragmentation et réassemblage (2)

- **Mécanisme d'émission d'une trame fragmentée**



Fragmentation et réassemblage (3)

- **Émission d'une trame fragmentée avec réservation du support**



Fragmentation et réassemblage (4)

- Deux champs permettent le réassemblage des fragments par la station destination :
  - ***Sequence control*** : permet le réassemblage de la trame grâce à
    - ***Sequence number*** : chaque fragment issu d'une même trame possède le même numéro de séquence
    - ***Fragment number*** : chaque fragment d'une même trame se voit attribuer un numéro de fragment, à partir de zéro, incrémenté pour chaque nouveau fragment
  - ***More fragment*** : permet d'indiquer si d'autres fragments suivent ; égale zéro si le fragment en cours est le dernier fragment

Variation du débit

- Débit compris entre 1 et 54 Mbps (802.11g)
- Différence due
  - aux en-têtes des trames utilisées
  - à certains mécanismes de fiabilisation de la transmission
  - un part importante du débit sert à la gestion de la transmission

- L'overhead engendré est plus important que les données elles-mêmes

Variation du débit

- Variable Rate Shifting :
  - ❖ permet de faire varier le débit d'une station en fonction de la qualité de la liaison
  - ❖ Permet à toutes les stations d'avoir un accès, même minimal, au réseau
  - ❖ Exple pour 802.11b: Débits possibles = 11 - 5,5 - 2 – 1 Mbits/s

Vitesse (Mbits/s)	Portée à l'intérieur	Portée à l'extérieur
11	50 m	200 m
5,5	75 m	300 m
2	100 m	400 m
1	150 m	500 m

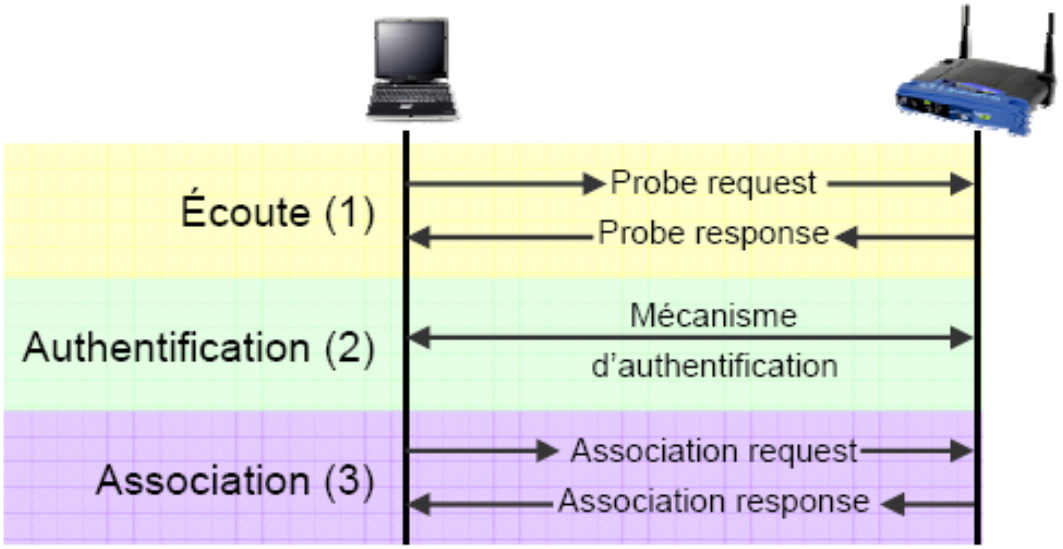
Gestion de la mobilité (1)

- Des trames balises permettent aux stations mobiles de rester synchronisées
- Procédure d'association-réassociation :
  - choix du point d'accès : puissance du signal, taux d'erreur, charge
  - écoute du support
    - **passive** : attente d'une trame balise
    - **active** : envoie d'une trame de requête (*Probe Request Frame*) et attente de la réponse contenant les caractéristiques du point d'accès
  - authentification : deux mécanismes
    - ***open system authentication*** : mode par défaut ; ne constitue pas un réelle authentification
    - ***shared key authentication*** : véritable mécanisme d'authentification, repose sur le WEP (*Wired Equivalent Privacy*) ; repose sur une clef secrète partagée
- Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)

Gestion de la mobilité (2)

Association

- utilisation d'un identifiant : SSID (*Service Set ID*) qui définit le réseau
- SSID émis régulièrement en clair par l'AP dans une trame balise : constitue une faille de sécurité



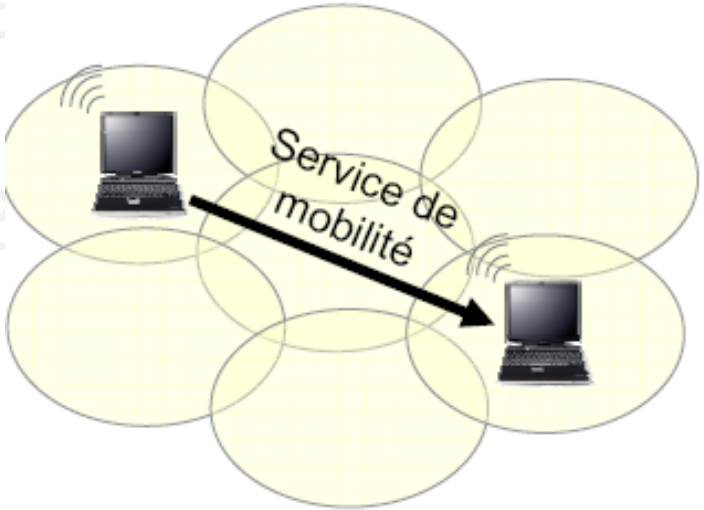
Réassociation

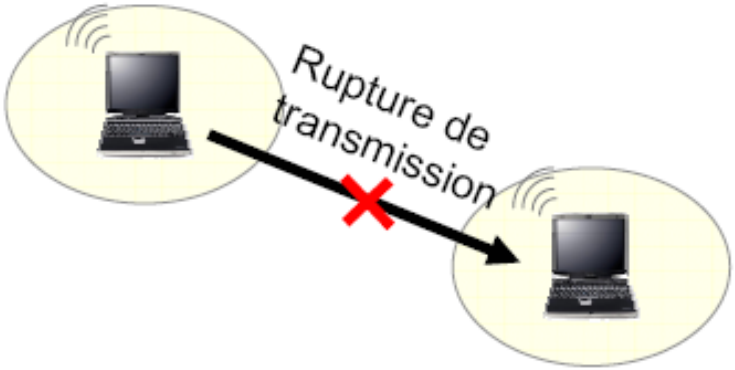
- similaire à l'association, effectuée lors de changements des caractéristiques de l'environnement (déplacement, trafic élevé)

Gestion de la mobilité (3)

Les handovers

- mécanisme permettant à un dispositif mobile de changer de cellule sans que la transmission en cours ne soit interrompue
- possible que si les cellules voisines se recouvrent
- non défini dans la norme IEEE 802.11 ni 802.11b (WiFi)

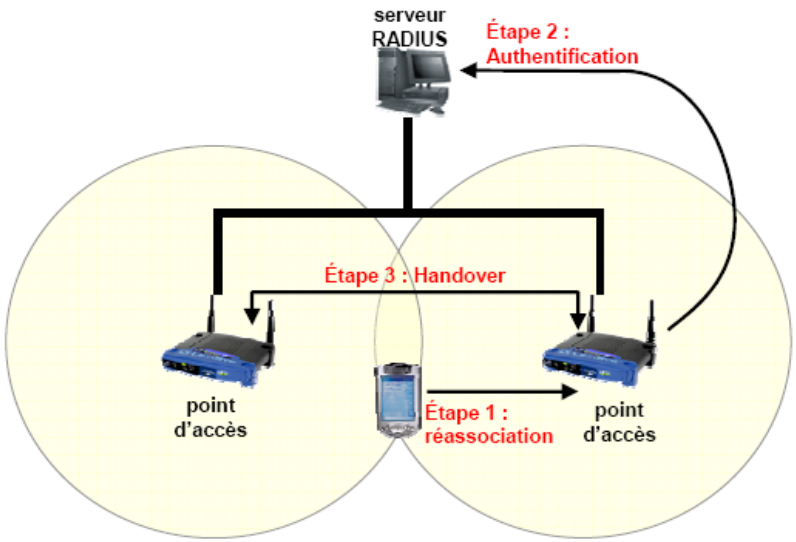




Gestion de la mobilité (4)

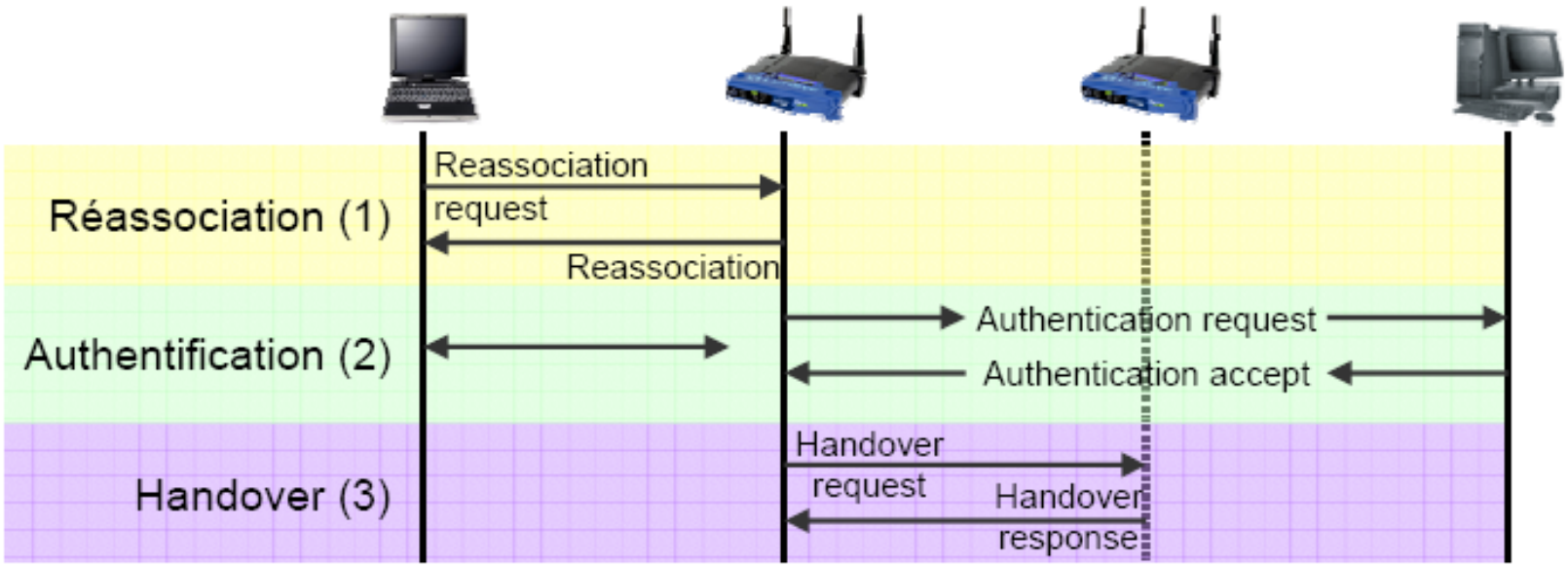
Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)

- défini à l'origine par Lucent puis intégré à la norme 802.11
- protocole de niveau transport (couche 4) qui se place au-dessus de UDP (*User Datagram Protocol*) : protocole sans connexion
- utilise le protocole RADIUS pour permettre des handovers sécurisés (RADIUS : *Remote Authentication Dial-In User Server*)
- serveur centralisé ayant une vue globale du réseau : il connaît la correspondance entre adresses IP et MAC



Gestion de la mobilité (5)

Protocole IAPP : *Inter-Access Point Protocol* (IEEE 802.11f)



Economie d'énergie

Stations mobiles : optimiser l'utilisation de l'énergie disponible :

- ***continuous aware mode*** : mode par défaut, pas d'économie d'énergie
- ***power save polling mode*** : mode économie d'énergie
  - le point d'accès tient un enregistrement de toutes les stations en mode économie d'énergie
  - il stocke toutes les données qui leur sont adressées
  - régulièrement, les stations s'éveillent pour recevoir un trame balise indiquant si oui ou non des données leur sont adressées
  - si oui, les stations récupèrent leurs données puis retournent en mode veille jusqu'à la prochaine trame balise

La sécurité

Introduction

- Une grande capacité de propagation des ondes radio-électriques
- Portée de propagation relativement grande
- Difficile de confiner les émissions dans un périmètre restreint

  → Conséquences : facilité que peut avoir une personne non autorisée d'écouter le réseau, éventuellement en dehors de l'enceinte du bâtiment où le réseau sans fil est déployé

Les risques en matière de sécurité

Les risque liés à la mauvaise protection d'un réseau sans fil sont multiples :

- L'interception de données consistant à écouter les transmissions des différents utilisateurs du réseau sans fil,
- Le détournement de connexion dont le but est d'obtenir l'accès à un réseau local ou à Internet,
- Le brouillage des transmissions consistant à émettre des signaux radio de telle manière à produire des interférences,
- Les dénis de service rendant le réseau inutilisable en envoyant des commandes factices.

L'interception de données

- Par défaut un réseau sans fil est non sécurisé, c'est-à-dire qu'il est ouvert à tous et que toute personne se trouvant dans le rayon de portée d'un point d'accès peut potentiellement écouter toutes les communications circulant sur le réseau.
- Pour un particulier la menace est faible car les données sont rarement confidentielles, si ce n'est les données à caractère personnel.
- Pour une entreprise l'enjeu stratégique peut être très important.

L'intrusion réseau

- Lorsqu'un point d'accès est installé sur le réseau local, il permet aux stations d'accéder au réseau filaire et éventuellement à internet si le réseau local y est relié. Un réseau sans fil non sécurisé représente de cette façon un point d'entrée royal pour le pirate au réseau interne d'une entreprise ou une organisation.
- Outre le vol ou la destruction d'informations présentes sur le réseau et l'accès à internet gratuit pour le pirate, le réseau sans fil peut également représenter une aubaine pour ce dernier dans le but de mener des attaques sur Internet.

  →En effet étant donné qu'il n'y a aucun moyen d'identifier le pirate sur le réseau, l'entreprise ayant installé le réseau sans fil risque d'être tenue responsable de l'attaque.

Le brouillage radio

- Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisé dans le réseau sans fil.
- Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.

Les dénis de service (1)

- La méthode d'accès au réseau de la norme 802.11 est basé sur le protocole CSMA/CA, consistant à attendre que le réseau soit libre avant d'émettre.
- Une fois la connexion établie, une station doit s'associer à un point d'accès afin de pouvoir lui envoyer des paquets.
- Les méthodes d'accès au réseau et d'association sont connus, et donc il est simple pour un pirate d'envoyer des paquets demandant la désassociation de la station.

  → ***Il s'agit d'un déni de service***,

  c'est-à-dire d'envoyer des informations de telle manière à perturber volontairement le fonctionnement du réseau sans fil.

Les dénis de service (2)

- D'autre part, la connexion à des réseaux sans fil est consommatrice d'énergie. Même si les périphériques sans fil sont dotés de fonctionnalités leur permettant d'économiser le maximum d'énergie, un pirate peut éventuellement envoyer un grand nombre de données (chiffrées) à une machine de telle manière à la surcharger.
- En effet, un grand nombre de périphériques portables (assistant digital personnel, ordinateur portable, ...) possèdent une autonomie limitée, c'est pourquoi un pirate peut vouloir provoquer une surconsommation d'énergie de telle manière à rendre l'appareil temporairement inutilisable, c'est ce que l'on appelle un déni de service sur batterie.

Les failles de sécurité

WiFi comporte de nombreuses failles dans toutes ses composantes « *sécurité* » :

- SSID (*Service Set ID*) :
  - transmis en clair par l'AP
  - le mécanisme *closed network* interdit sa transmission dans les balises
  - en mode ad-hoc, le SSID est systématiquement transmis en clair
  - même en mode fermé, le SSID est transmis en clair pendant l'association
  - utilisation du SSID par défaut, configuré par les constructeurs
- ACL (Access Control List)
  - optionnel, donc peu souvent utilisé
  - repose sur l'identification de l'adresse MAC
  - il suffit de *sniffer* le réseau puis copier une adresse MAC
- WEP
  - algorithme de chiffrement robuste : clef différente pour chaque paquet
  - faiblesse du WEP : système de génération de la clef : le vecteur d'initialisation est souvent réinitialisé à zéro à chaque nouvelle transmission

Accès au réseau et chiffrement (1)

SSID : Service Set IDentifier (identifiant de réseau)

- Seul mécanisme de sécurité obligatoire
- Pour s'identifier auprés d'un AP, les clients d'un réseau 802.11 utilisent un SSID
- Sans algorithme de chiffrement, l'ID de réseau n'est pas crypté lors de la transmission des trames
- Il est facile qu'un intrus obtienne le SSID lui permettant d'accéder au réseau
- Le protocole de chiffrement WEP par exemple a été mis en place, mais il n'est pas suffisant
- Autres précautions :
  - Supprimer la configuration par défaut des AP en modifiant la clef WEP si elle est activée et l'ID réseau (SSID) installé par défaut
  - Protéger ou désactiver les services d'administration fournis avec l'interface
  - Réduire la puissance d'émission de l'AP au minimum nécessaire afin de diminuer le rayonnement des ondes (il est tjs possible d'écouter le canal mais avec plus de complexité)
  - Il est aussi possible de filtrer les @ MAC ayant le droit de communiquer avec le pont
    (à l'aide d'un sniffer, il est possible de récupérer le trafic échangé entre deux machines et simuler une adresse MAC décodée)

Accès au réseau et chiffrement (2)

ACL (Access Control List)

- Liste maintenue par le point d'accès
- Contient les adresses MAC autorisées à se connecter à cet AP
- Optionnelle et peu utilisée car peu fiable

Accès au réseau et chiffrement (3)

WEP (Wired Equivalent Privacy)

- Basé sur des clés de cryptage partagées interdisant l'accès à toutes les personnes ne connaissant pas ce mot de passe
- Chaque périphérique 802.11 utilise une clé, soit un mot de passe, soit une clé dérivée de ce mot de passe
- La faille de sécurité du WEP : provient du mode de fonctionnement de **l'algorithme de chiffrement (RC4) qui permet à tout décodeur de déduire** certaines informations menant à la reconstitution de la clé.
- Il est toutefois possible de dissuader les intrus en multipliant les obstacles devant eux. Des protocoles de sécurité tels que **IPSec, SSL ou SSH** ne sont pas facilement vulnérables

Accès au réseau et chiffrement (4)

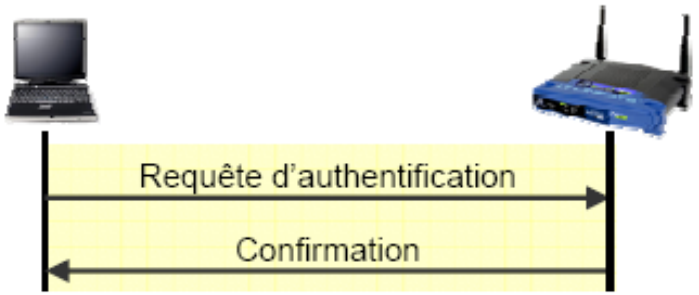
WPA (Wi-Fi Protected Access)

- repose sur un système **d'échange de clés dynamiques, renouvelées tous les 10 ko de données**
- Procédé, appelé **TKIP (*Temporal Key Integrity Protocol)***
- Protège mieux les clés du décryptage et devrait améliorer sensiblement la sécurité des réseaux sans fil même si l'algorithme utilisé reste inchangé

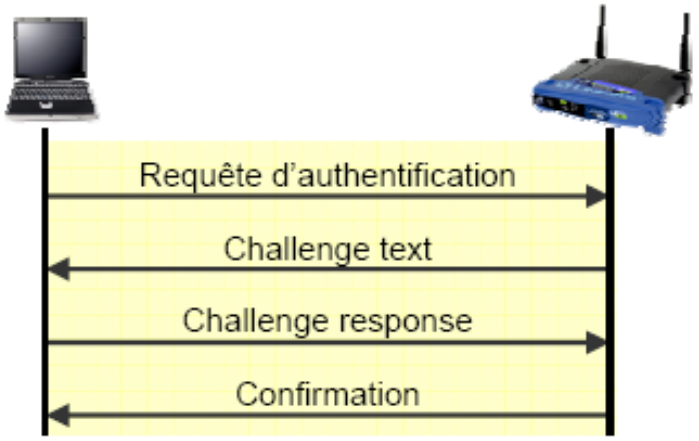
Authentification

2 mécanismes :

- ***Open system Authentication*** : mécanisme par défaut



- ***Shared Key Authentication*** :



Les solutions :
Une infrastructure adaptée

- Lors de la mise en place d'un réseau sans fil **positionner intelligemment les points d'accès** selon la zone que l'on souhaite couvrir.
- Eviter les murs extérieurs mais choisir plutôt un emplacement central.
- En se promenant autour de l'immeuble, **on peut établir le périmètre** à l'intérieur duquel la borne est accessible.
- Il n'est toutefois pas rare que la zone effectivement couverte soit largement plus grande que souhaitée, auquel cas il est possible de **réduire la puissance de la borne d'accès afin** d'adapter sa portée à la zone à couvrir.

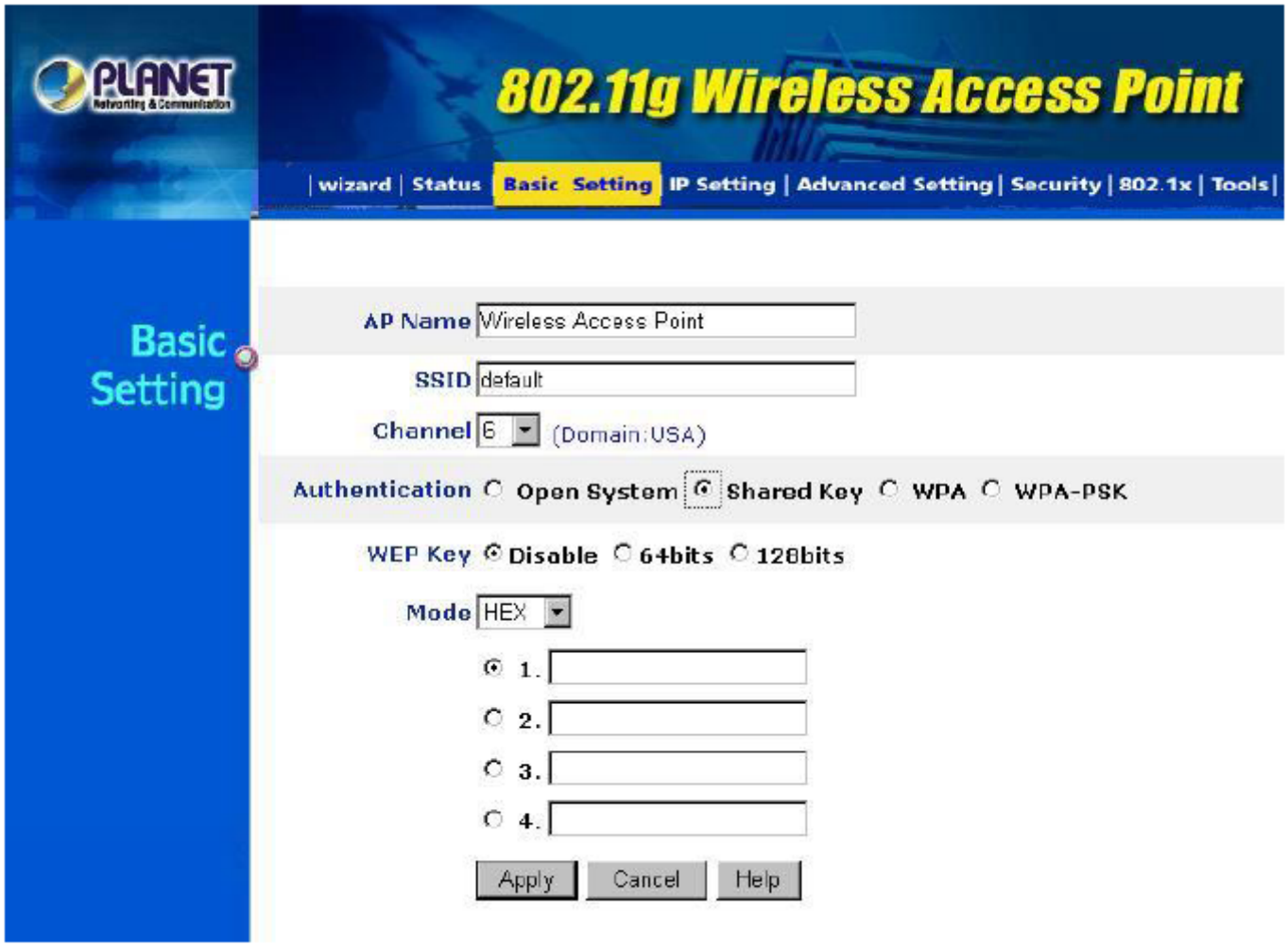
Les solutions :
Eviter les valeurs par défaut (1)

- Lors de la première installation d'un point d'accès, celui-ci est configuré avec des valeurs par défaut, y compris en ce qui concerne le **mot de passe de l'administrateur.**
- Un grand nombre d'administrateurs considèrent qu'à partir du moment où le réseau fonctionne il est inutile de modifier la configuration du point d'accès.
- Toutefois les paramètres par défaut sont tels que la sécurité est minimale. Il est donc impératif de se connecter à l'interface d'administration (généralement via une interface web sur un port spécifique de la borne d'accès) notamment pour définir un mot de passe d'administration.

Les solutions :
Eviter les valeurs par défaut (2)

- Afin de se connecter à un point d'accès il est indispensable de connaître l'identifiant du réseau (SSID).
- Ainsi il est vivement conseillé de modifier le nom du réseau par défaut et de désactiver la diffusion (SSID broadcast: diffusion du nom SSID) de ce dernier sur le réseau.
- Le changement de l'identifiant réseau par défaut est d'autant plus important qu'il peut donner aux pirates des éléments d'information sur la marque ou le modèle du point d'accès utilisé. L'idéal est même de modifiez régulièrement le nom SSID!
- Il faudrait même éviter de choisir des mots reprenant l'identité de l'entreprise ou sa localisation, qui sont susceptibles d'être plus facilement devinés.

Les solutions :
Activer le cryptage WEP ou WPA



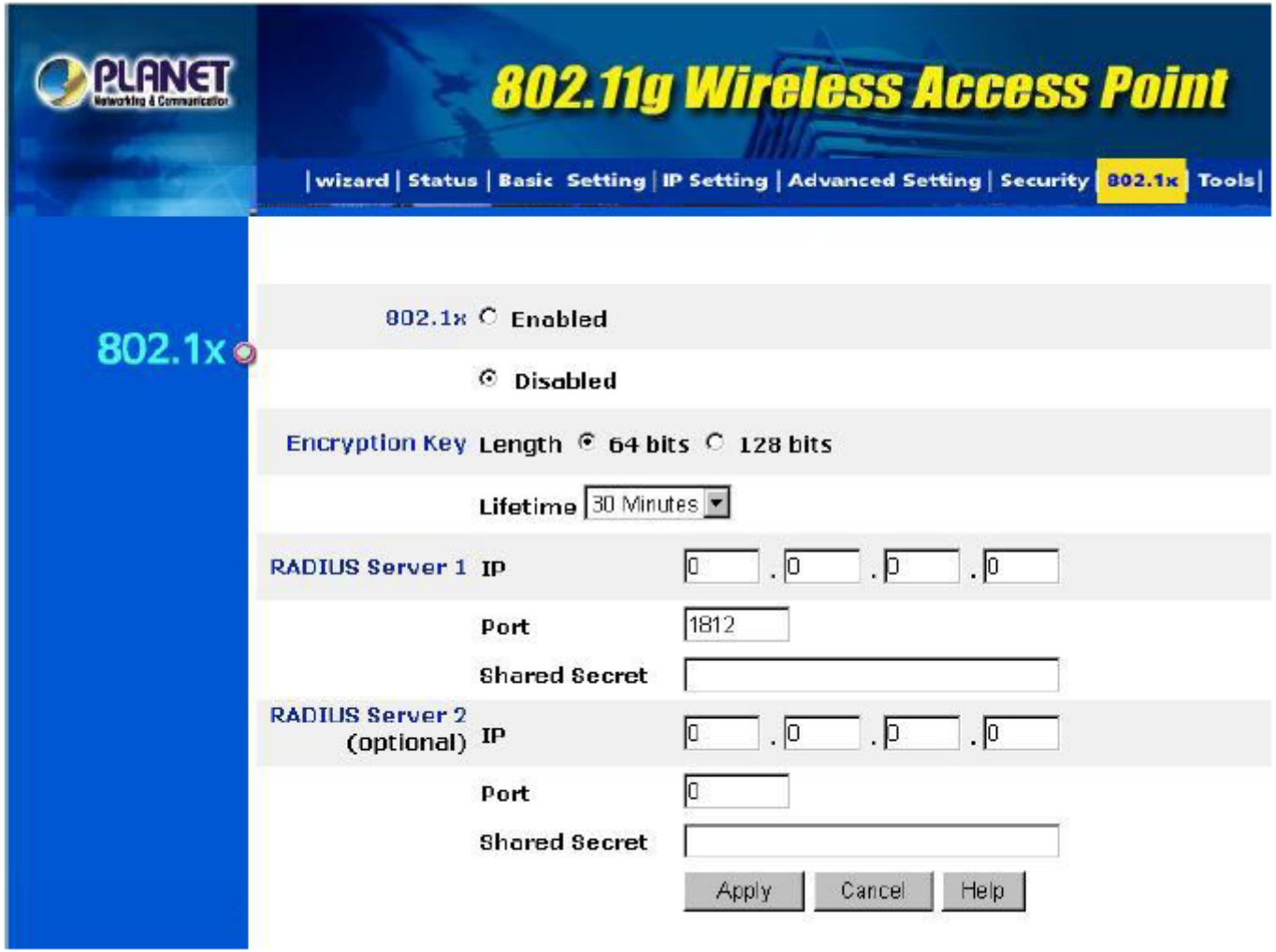
Les solutions :
Le filtrage des adresses MAC

- Chaque adaptateur réseau possède une adresse physique qui lui est propre (adresse MAC). Les points d'accès permettent généralement dans leur interface de configuration de gérer une liste de droits d'accès (appelée ACL) basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil.
- En activant ce MAC Address Filtering (Filtrage des adresses MAC), même si cette précaution est un peu contraignante, cela permet de limiter l'accès au réseau à un certain nombre de machines.
- En contrepartie cela ne résout pas le problème de la confidentialité des échanges.

Les solutions :
Améliorer l'authentification (1)

- Afin de gérer plus efficacement les authentifications, les autorisations et la gestion des comptes utilisateurs (en anglais AAS pour *Authentication, Authorization, and Accounting) il* est possible de recourir à un **serveur RADIUS (*Remote Authentication Dial-In User Service).***
- Le protocole RADIUS (défini par les RFC 2865 et 2866), est un système client/serveur permettant de gérer de façon centralisée les comptes des utilisateurs et les droits d'accès associés.

Les solutions :
Améliorer l'authentification (2)



Les solutions :
Mise en place d'un VPN

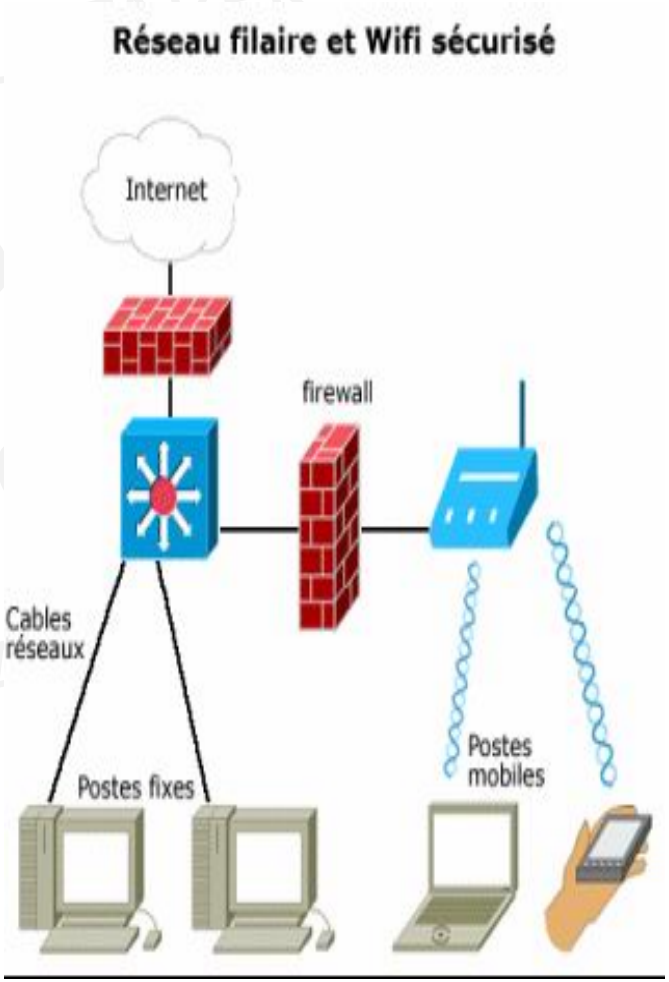
Pour connecter les utilisateurs nomades se branchant au réseau par le biais d'une borne publique, et pour toutes les communications nécessitant un haut niveau de sécurisation, il faut mettre en place un **réseau privé virtuel (VPN) qui offrira un bon niveau de sécurité et** empêchera la plupart des intrusions indésirables.

Les solutions :
Définir des adresses IP fixes

Les risques d'intrusion externes sont bien moindres en attribuant des a**dresses IP fixes aux stations de la flotte bénéficiant d'une connexion sans fil. Il est ainsi possible de gérer une** table d'adresses des connexions autorisées. Il faut, dans ce cas, **désactiver la fonction DHCP** au niveau du serveur auquel est connectée la borne WiFi.

Les solutions :
Installer un pare-feu

- On peut aussi installez un **firewall comme si le point** d'accès était une connexion internet.
- Ce firewall peut être le serveur **IPsec (VPN) des clients sans fils.**
- Un réseau WiFi "sécurisé" peut se schématiser comme cela. On considère ici que tout le réseau WiFi est étranger au réseau local, au même titre qu'Internet.
- L'utilisation d'un pare-feu (firewall) comme pour la connexion Internet, permet de filtrer les adresses MAC associé à des adresses IP fixes.
- Dans le cas du VPN, le firewall ou un serveur derrière ce dernier fait office de terminal VPN.
- Certains points d'accès proposent des "petits" firewall permettant de faire un filtrage de plus sur les clients de votre réseau.

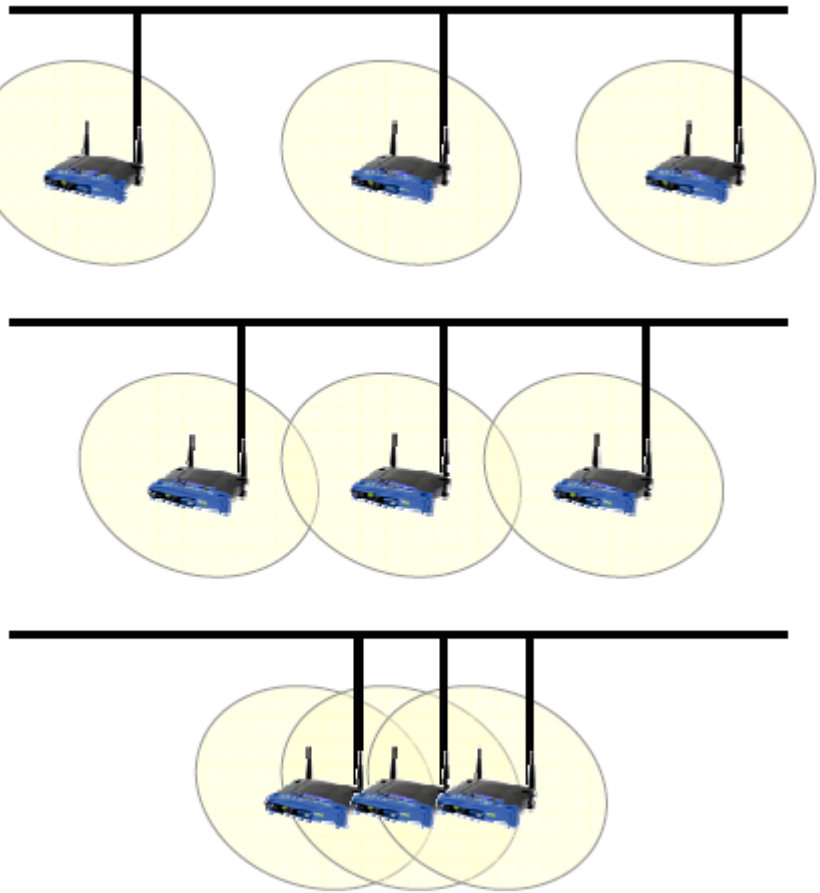


Les solutions

- Chacun est libre de modifier ces règles en ajoutant des couches supplémentaires.
- Le futur protocole IP ipv6 contient dans ses paquets la sécurisation ipsec.
- L'ipv6 peut être utilisé en WiFi si les clients gèrent l'ipv6,
- Actuellement tous les Linux, Unix ont une pile ipv6 fonctionnelle
- Sur Windows 2000 et XP l'ipv6 est activable et utilisable
- Déjà proposé par défaut dans les nouvelles versions.

Configuration et Installation

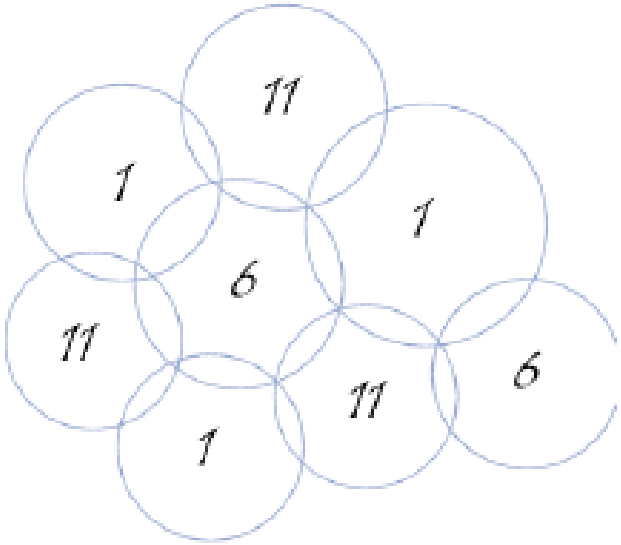
Choix de la topologie

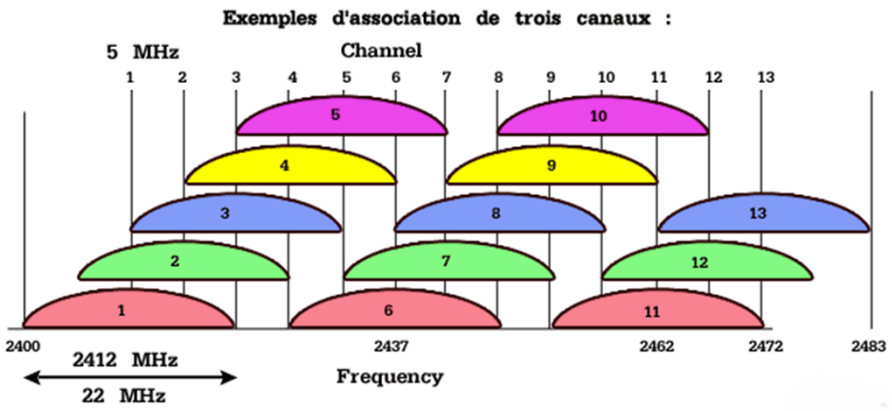


- **les cellules sont disjointes**
  - faible nombre de canaux
  - pas d'interférence
  - pas de mobilité
- **les cellules se recouvrent**
  - réseaux sans fils
  - service de mobilité
  - exploitation de l'espace
  - gestion de l'affectation
- **les cellules se recouvrent mutuellement**
  - configuration des canaux nécessaire
  - nombre important d'utilisateurs

Installation

- si deux points d'accès utilisant les mêmes canaux ont des zones d'émission qui se recoupent, des distortions du signal risquent de perturber la transmission.
- Pour éviter toute interférence il est recommandé d'organiser la répartition des points d'accès et l'utilisation des canaux de telle manière à ne pas avoir deux points d'accès utilisant les mêmes canaux proches l'un de l'autre.





Modes opérationnels des points d'accès : Mode point d'accès

- Les nœuds doivent trouver les points d'accès les plus proches pour communiquer avec un autre AP ou une réseau filaire Ethernet

Modes opérationnels des points d'accès : Mode Client AP sans fil

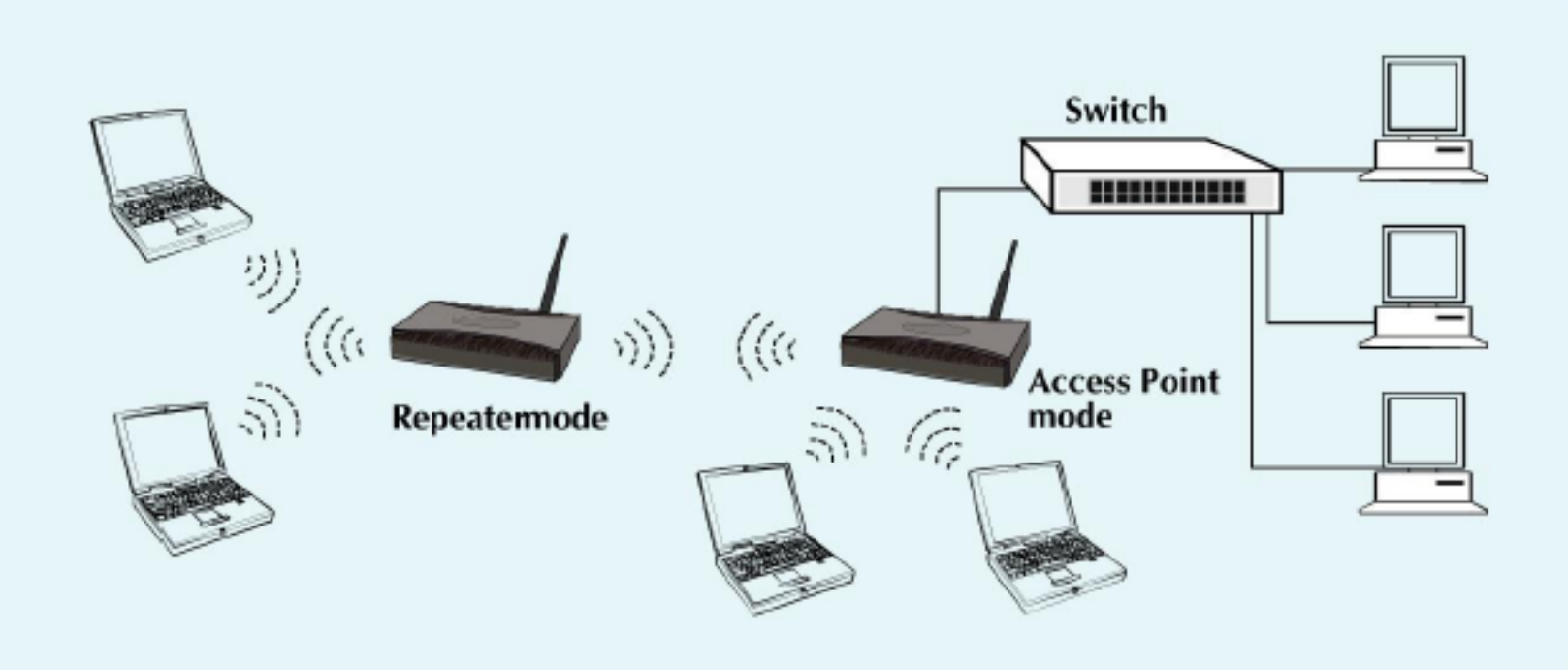
- Appliqué si les nœuds désirent de se connecter là où il n'y a pas de liaisons filaires

Modes opérationnels des points d'accès : Mode Pont sans fil

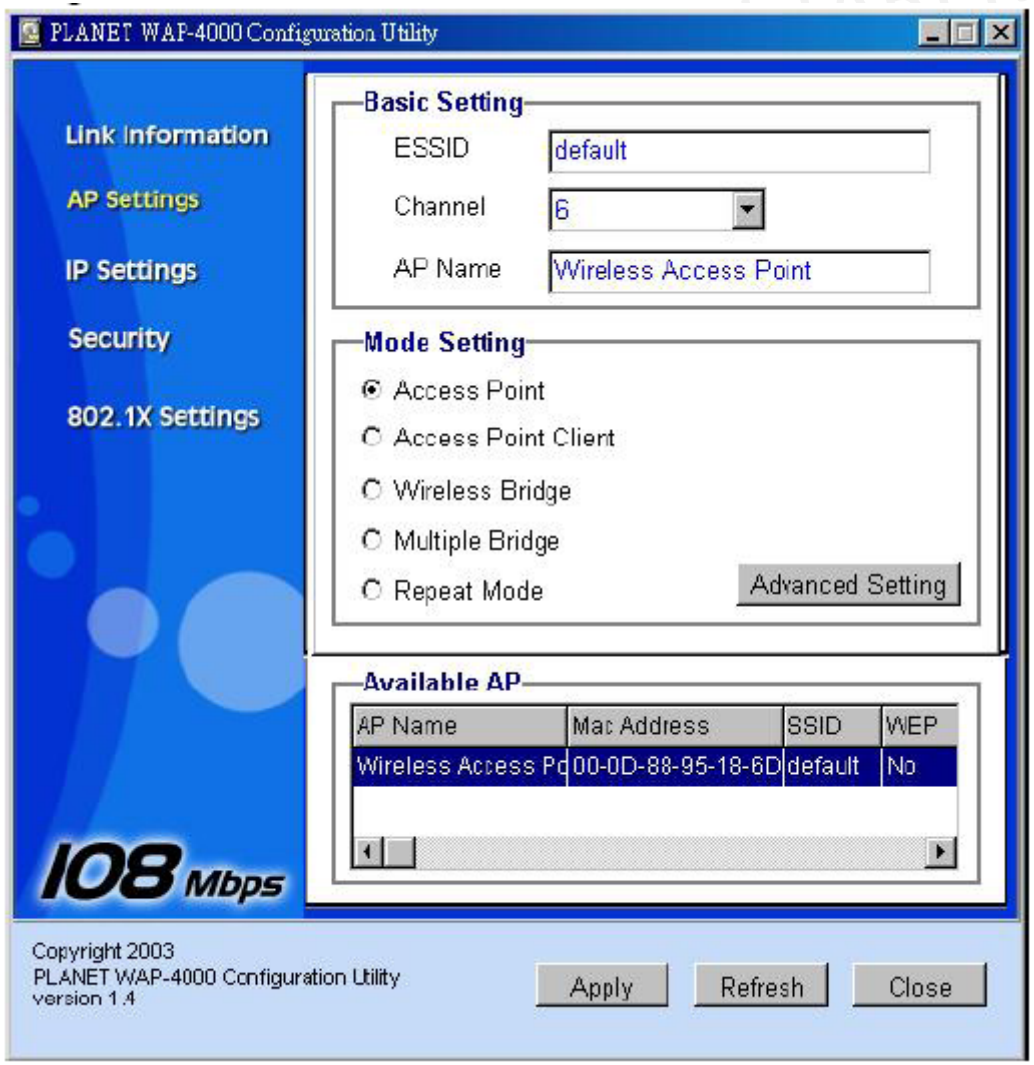
- Appliqué si impossibilité de réaliser une connexion filaire entre les deux segments du réseau

Modes opérationnels des points d’accès : Mode multi-Ponts sans fil

Modes opérationnels des points d’accès : Mode Répéteur



Modes opérationnels des points d'accès : Le choix



Bibliographie

- CisComag, Juin 2009
- Camille Diou, « WLAN : les réseaux sans fils et WFI », LICM, Université de Metz
- Davor Males & Guy Pujolle, « WiFi par la pratique », Eyrolles 2002
- P. Ciurlik, N. Engrand, S. Marszalek, X. Okoué,
  « WiFi & Bluetooth », USTL
- Planet, MAP-400 User's Manual