UFR SET

Technologies des réseaux sans fil

Enseignant: Mr **Abdoulaye DOUMBOUYA**
Ingénieur en Réseaux & Télécoms

contact: abdoulayedoumbouya@gmail.com

Plan de la présentation

1. Les réseaux locaux sans fil
2. Concepts des RLSF
3. Déploiements des RLSF
4. Sécurité des réseaux locaux sans fil
5. Dépannage des RLSF

I. Les réseaux locaux sans fil

Les objectifs

- Décrire les composants et le fonctionnement de base des réseaux locaux sans fil
- Décrire les composants et le fonctionnement de la sécurité de base des réseaux locaux sans fil
- Configurer et vérifier l'accès de base aux réseaux locaux sans fil
- Résoudre les problèmes d'accès aux clients sans fil

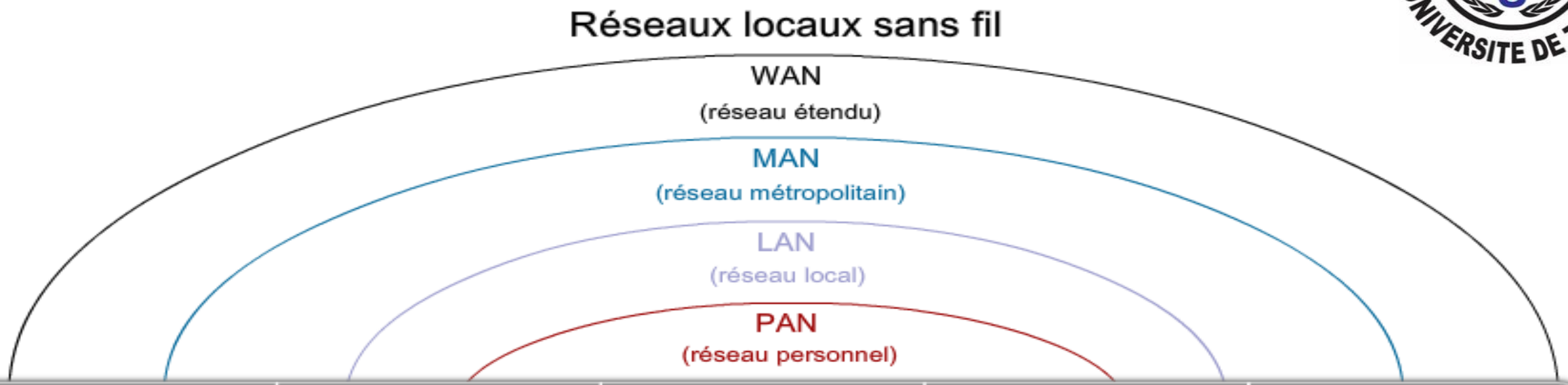
Pourquoi les réseaux locaux sans fil ont-ils autant de succès ?

Les motivations principales

- Abréviation RLSF ou WLAN
- Faciliter le câblage et le déploiement des équipements
- Réduire les coûts de câblage généralement onéreux
- Faciliter la mobilité des utilisateurs
- Création des réseaux spontanés sans l'apport d'une entité particulière

II. Concepts des RLSF

Les différents types de RLSF



	PAN	LAN	MAN	WAN
Normes	Bluetooth 802.15.3	802.11	802.11 802.16 802.20	GSM, CDMA, Satellite
Vitesse	< 1 Mbits/s	De 11 à 54 Mbits/s	10-100+ Mbits/s	10 Kbits/s-2 Mbits/s
Portée	Courte	Moyenne	Moyenne-Longue	Longue
Applications	Peer to peer Périphérique à périphérique	Réseaux d'entreprise	Accès à la boucle locale	Périphériques de données mobiles

Différence WLAN / WMAN

- Les WLAN sont locaux
  - Portée d'un immeuble ou d'un campus
- Radio ou infrarouge
- Pas besoin de licence d'utilisation des fréquences
  - Bande ISM
- Equipements propres aux utilisateurs
  - Borne sans fil

- Les WMAN sont métropolitains
  - Portée d'une ville, pays
- Transmission par réseaux cellulaires
- Besoin de licence pour les fréquences
- Equipements propres aux opérateurs
- Terminal chez le client
  - Ex : GSM, GPRS, EDGE, UMTS

Comparaison entre un réseau local sans fil et un réseau local filaire

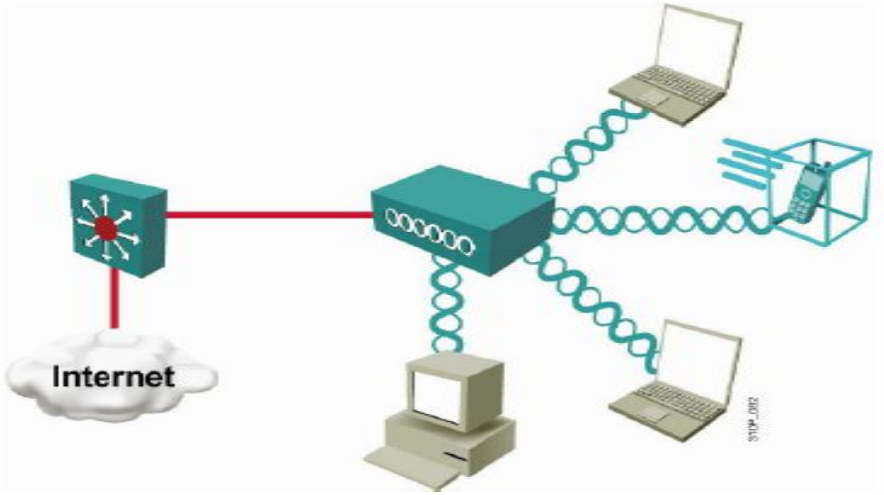
Caractéristique	Réseau local sans fil 802.11	Réseaux locaux Ethernet 802.3
Couche physique	Radiofréquence (RF)	Câble
Accès aux supports	Évitement de collision	Détection de collisions
Disponibilité	Quiconque équipé d'une carte réseau radio dans la portée d'émission d'un point d'accès	Connexion par câble requise
Signaux parasites	Oui	Sans conséquence
Réglementation	Autres réglementations édictées par les autorités locales	Norme IEEE

Contraintes des RLSF

- Bande passante
  - Partage de l'accès au canal sur une même fréquence
- Signal radio
  - Atténuation avec la distance (Indoor et Outdoor)
- Interférences radios
  - Par des fréquences trop proches (signal instable)
- SNR
  - Empêche le décodage si valeur faible
- Energie
  - Limitée (Emission, réception et écoute de porteuse consomment de l'énergie)

RLSF ou WLAN

- Réseaux partagés
- Point d'accès
  - Fonctionne comme un hub Ethernet
- Les données sont transmises au travers des ondes radios
- Les communications se font de manière alternée
  - Mécanisme d'accès au médium CSMA/CA
- La même bande de fréquence est utilisée pour la transmission et la réception
  - Cependant, utilisation de plusieurs porteuses dans la bande de fréquence (Interférences)



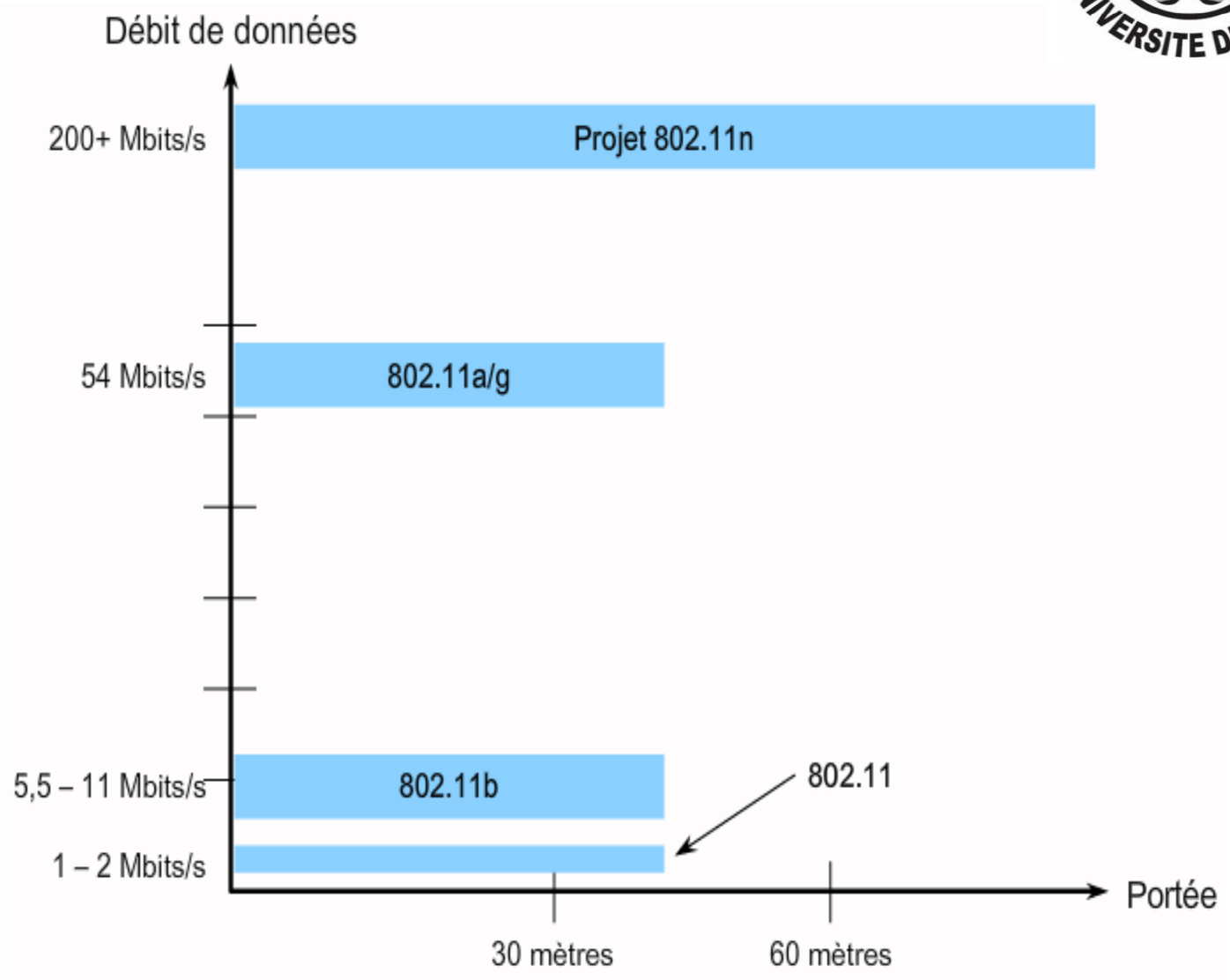
Normes des réseaux locaux sans fil

La norme 802.11 relative aux RSLF est une norme IEEE qui définit la façon dont les radiofréquences (RF) sont utilisées pour la couche physique et la sous-couche MAC des liaisons sans fil.

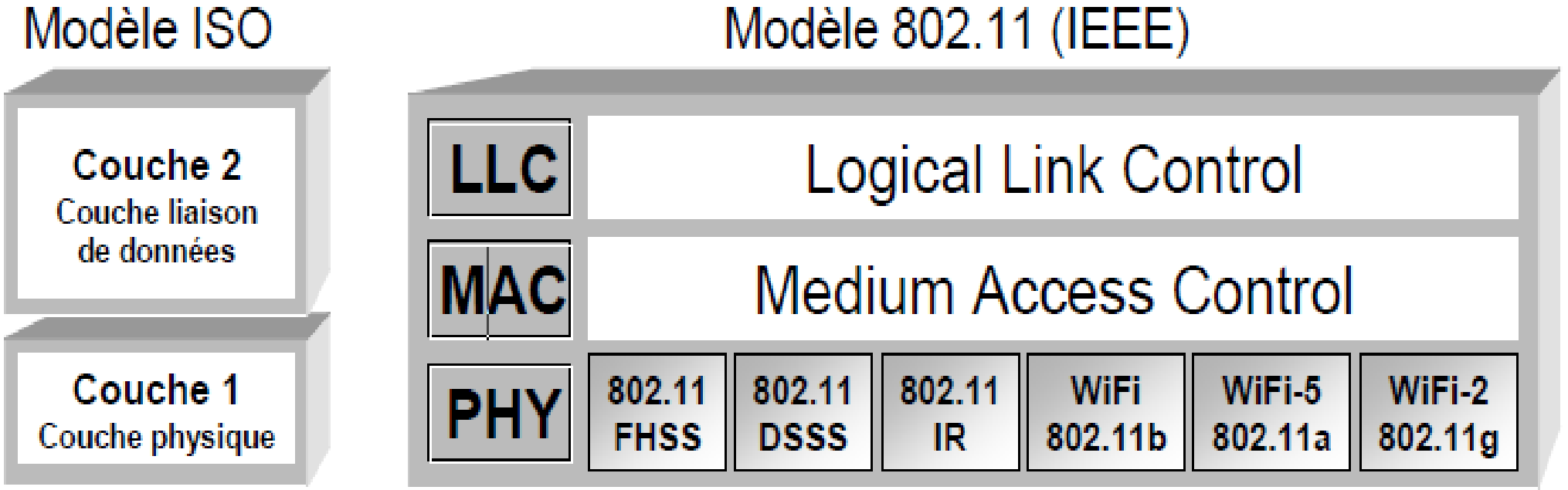
	802.11a	802.11b	802.11g		802.11n
Bande	5,7 GHz	2,4 GHz	2,4 GHz		À confirmer Bandes 2,4 et 5 GHz (probablement)
Canaux*	Jusqu'à 23	3	3		
Modulation	OFDM	DSSS	DSSS	OFDM	MIMO-OFDM
Débits de données	Jusqu'à 54 Mbits/s	Jusqu'à 11 Mbits/s	Jusqu'à 11 Mbits/s	Jusqu'à 54 Mbits/s	248 Mbits/s supposés pour deux flux MIMO
Avantages	~35 mètres	~35 mètres	~35 mètres		~70 mètres
Inconvénients	Octobre 1999	Octobre 1999	Juin 2003		Ratification attendue en 2008
Avantages	Rapidité, moins sujette aux interférences	Faible coût, bonne portée	Rapidité, bonne portée, peu sensible aux obstacles		Excellents débits de données, portée accrue
Inconvénients	Coût plus élevé, portée inférieure	Lenteur, sujette aux interférences	Sujette aux interférences des appareils utilisant la bande 2,4 GHz		

Gestion des débits

- Zone de couverture
  - Puissance d'émission
  - Fréquence utilisée
- Atténuation du signal avec la distance
- Le débit chute en fonction de la distance
- Une AP de 11Mb/s peut voir son débit chuter jusqu'à 1Mb/s

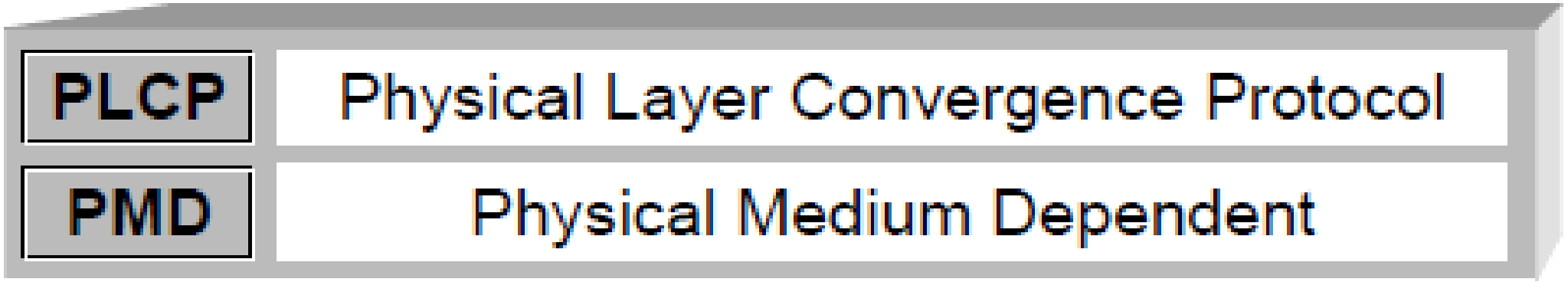


Architecture en couches



- Modele 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

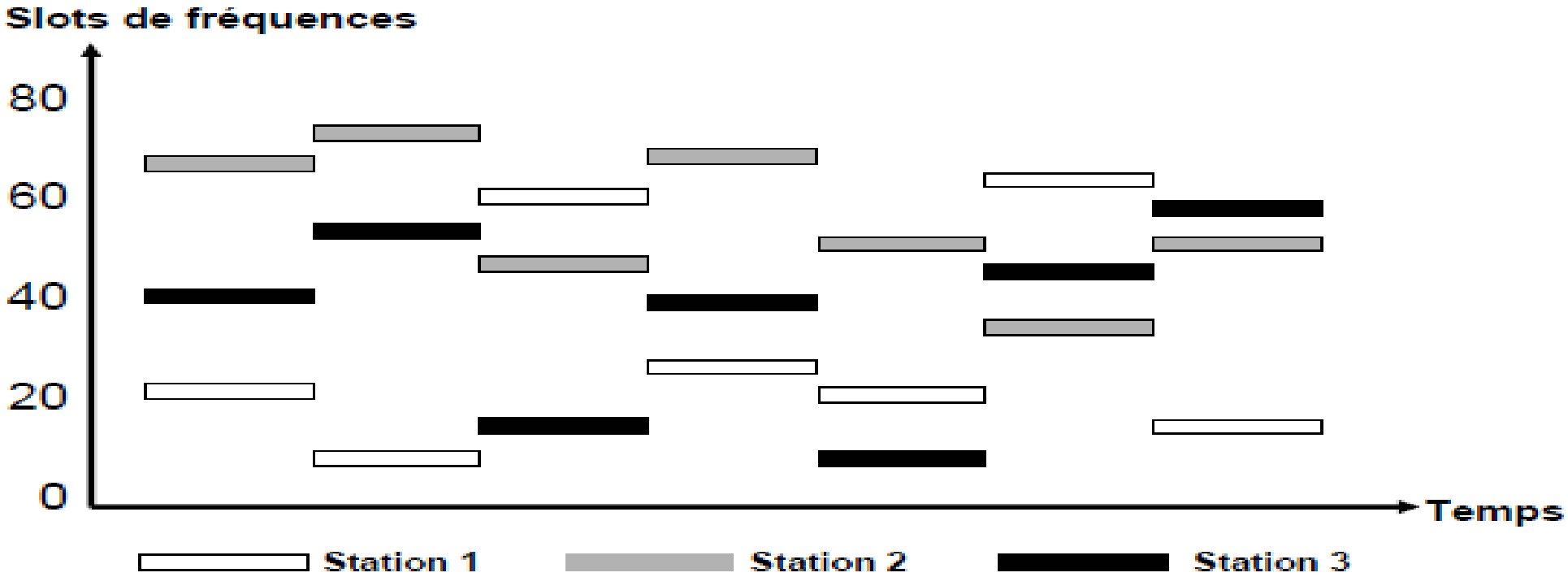


- Composée de deux sous-couches :
  - PMD gère l'encodage des données et de la modulation
  - PLCP gère l'écoute du support et signale à la couche MAC que le support est libre par un CCA (Clear Channel Assessment)

FHSS

Frequency Hopping Spread Spectrum

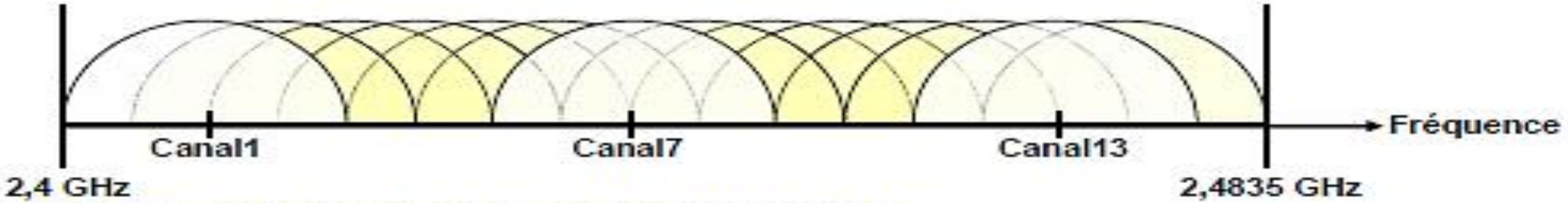
- 79 canaux de 1 MHz de largeur de bande
- 3 ensembles de 26 séquences, soit 78 séquences de sauts possibles
- Exemple : 3 stations sur 7 intervalles de temps : émission simultanée mais pas sur le même canal



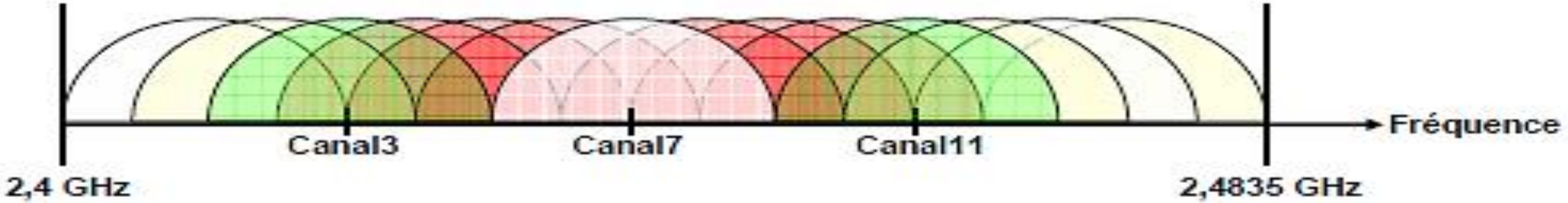
DSSS

Direct Sequence Spread Spectrum

- Technique la plus répandue aujourd'hui : 802.11b
- 14 canaux de 20 MHz
- Fréquences crête espacées de 5 MHz
  - canal 1 = 2,412 GHz ; canal 14 = 2,477 GHz



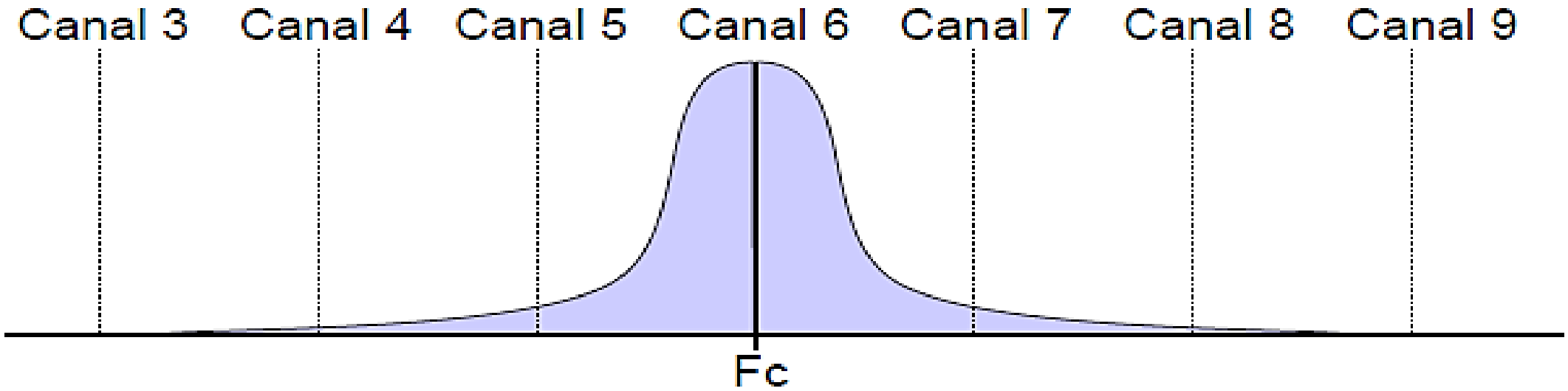
- Largeur totale de la bande = 83,5 MHz
- Canaux recouvrant : inexploitables simultanément



DSSS

Direct Sequence Spread Spectrum

- 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



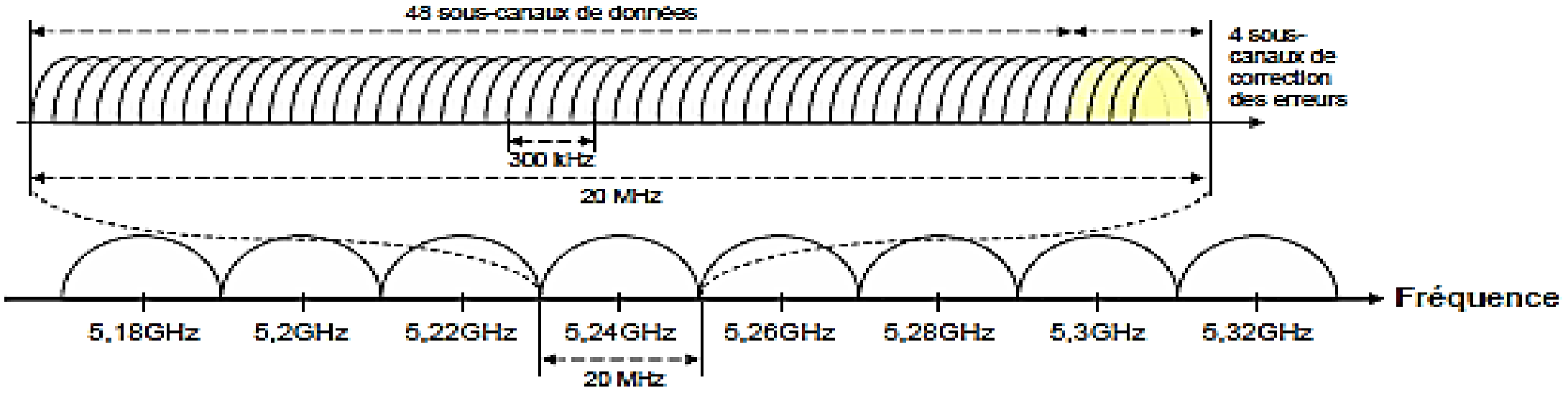
Spectre d'un canal

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

OFDM

Orthogonal Frequency Division Multiplexing

- bande U-NII (5 GHz)
- division des 2 premières sous-bandes en 8 canaux de 20 MHz
- 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



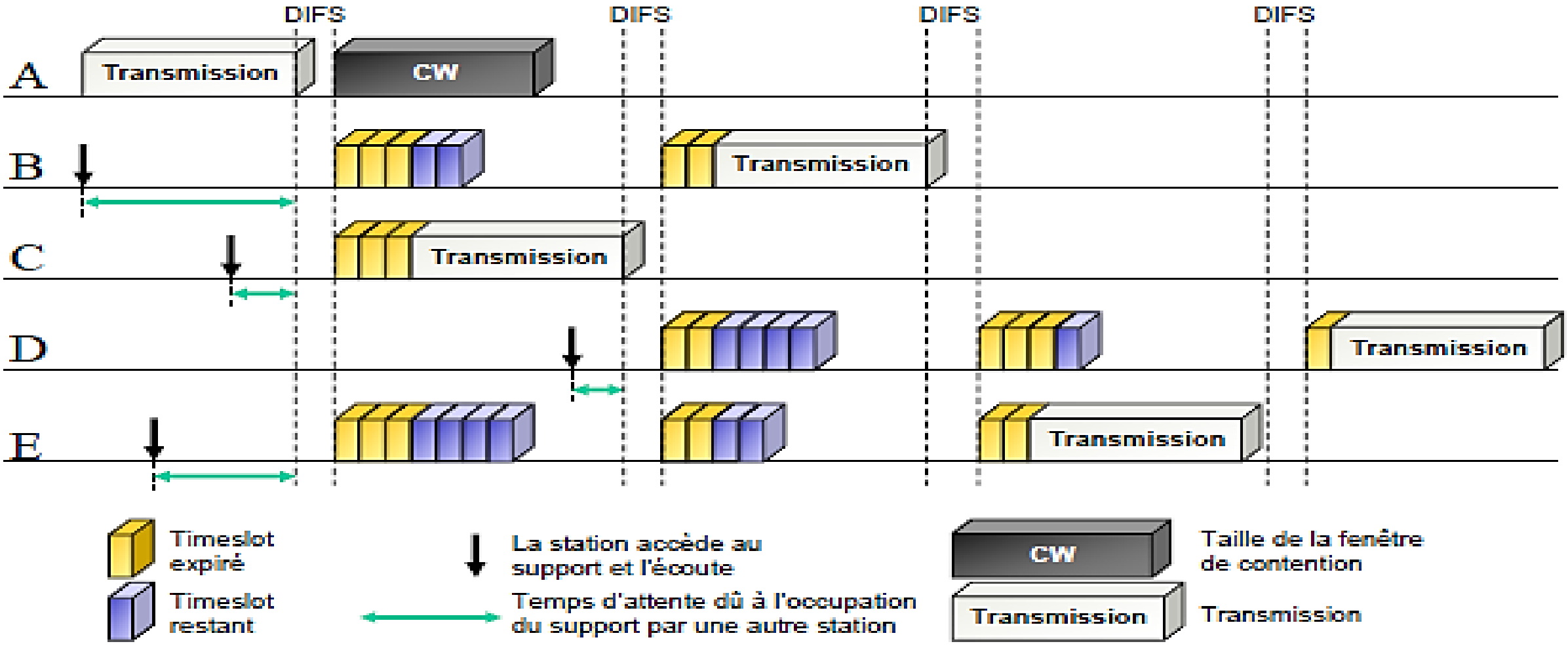
Mécanisme d'accès CSMA/CA

- Ecoute du support radio avant transmission
  - S'il est occupé la transmission est différée
  - Si le support est/ou redevient libre, alors la transmission est autorisée
- Risque pour que des stations émettent en même temps
  ➡ Collisions
- La détection d'une collision est repérée en cas de non réception d'un ACK au bout d'un timeout
- Les trames sont retransmises jusqu'à une limite
- Backoff avant la transmission d'une trame
- Backoff exponentiel en cas de collision

Backoff

Le *back-off*

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



Backoff

- Il se peut que deux stations qui détectent le canal libre en même temps, émettent également en même temps il se produit alors une collision. Dans ce cas chacune des stations va retransmettre après un temps aléatoire appelé

  ➡ backoff

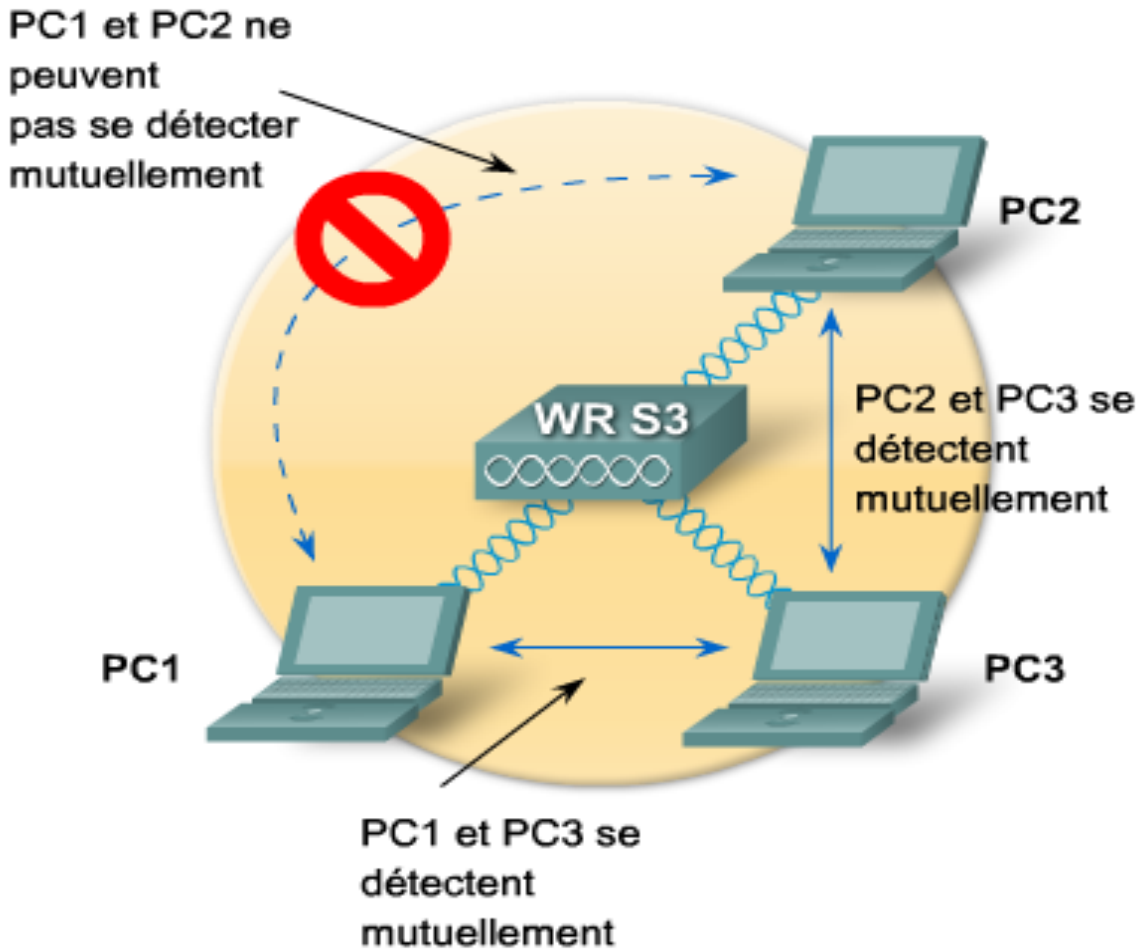
- Il est donc peut probable que ces stations choisissent le même temps aléatoire : évitement des collisions
- Ainsi, on est sur que la **station C** accédera au canal lorsque son backoff arrivera à la valeur 0

Nœud caché

Problème du nœud caché :

- PC1 et PC2 accèdent à Comm3 SF
- PC1 et PC2 ne peuvent pas s'atteindre mutuellement
- PC1 ne détecte pas l'activité de PC2 sur le canal
- PC1 envoie des données pendant que PC2 en transmet
- Une collision se produit

PC3 étant détecté à la fois par PC1 et PC2, aucune collision n'implique PC3.



La couche MAC

- Résous le problème du **nœud caché**
- Définit deux modes d'accès au canal radio :
  - Le mode PCF (Point Cordination Function) (pas de collision)
    - La station de base prend en charge les communications
  - Le mode DCF (Distributed Cordination Function) (Collision possible)
    - Utilisé par tous les mobiles
    - Accès équitable et probabiliste au canal radio
    - Pas de gestion centralisée des communications
    - Aussi bien pour le mode infrastructure que **ad hoc**
- Le mode DCF est le mode standard le plus répandu pour les réseaux IEEE 802.11

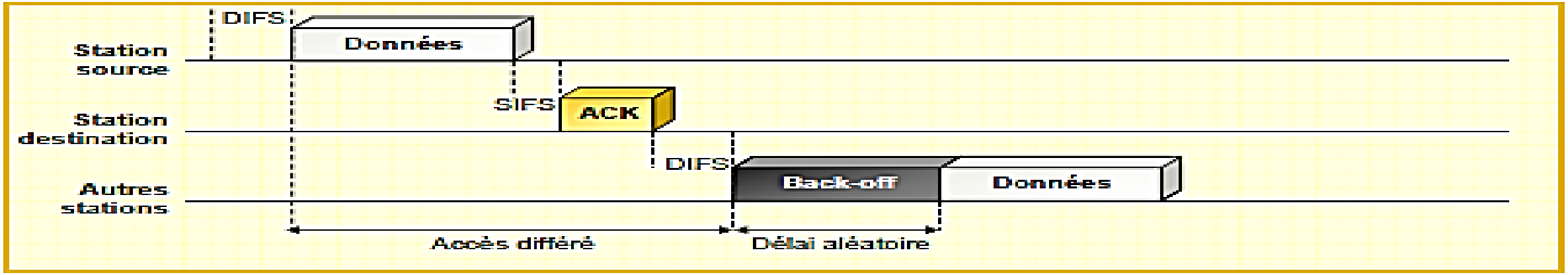
La couche MAC-DCF

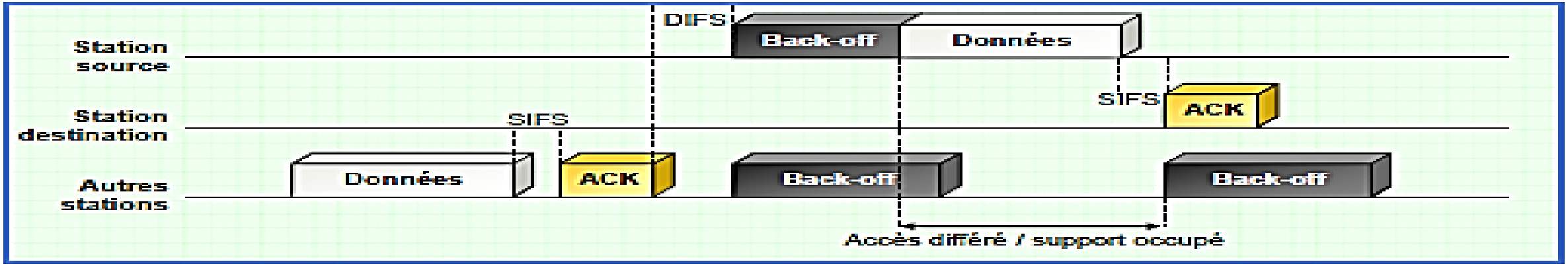
- Deux modes de transmission
  - Mode broadcast
  - Mode unicast
    - Un ACK est renvoyé par l'émetteur pour indiquer à la source la bonne réception de la trame
- IFS (Inter Frame Space) (Mécanisme d'espacement de trame)
  - DIFS : temps d'attente d'une station avant toute nouvelle transmission 50µs
  - SIFS : durée séparant la réception d'un paquet de données et l'envoi de son acquittement 10µs
  - EIFS : temps d'attente en cas d'écoute d'une transmission distante 364µs

La couche MAC-DCF

- IFS (Inter Frame Space) (Mécanisme d'espacement de trame)
  - DIFS : temps d'attente d'une station avant toute nouvelle transmission 50µs
  - SIFS : donne une priorité absolue à certains messages et notamment aux acquittements10µs

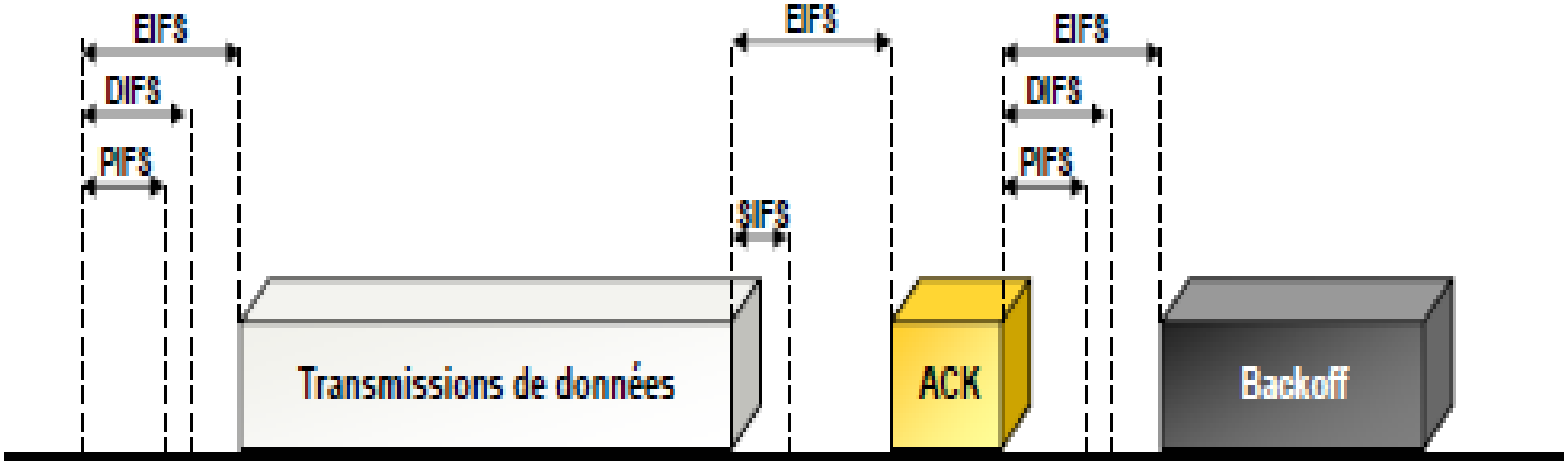
Exemples de transmissions





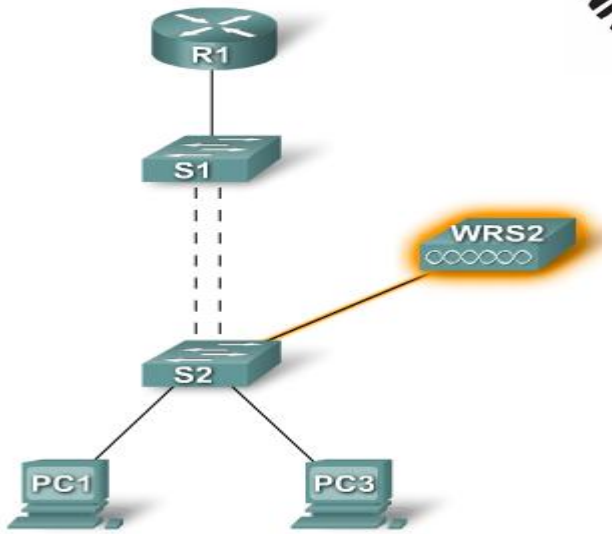
La couche MAC-DCF

- Le Point Coordination Function IFS (PIFS) est utilisé par les bornes d'accès pour l'émission de données qui disposent ainsi d'un accès prioritaire par rapport à l'émission des stations,

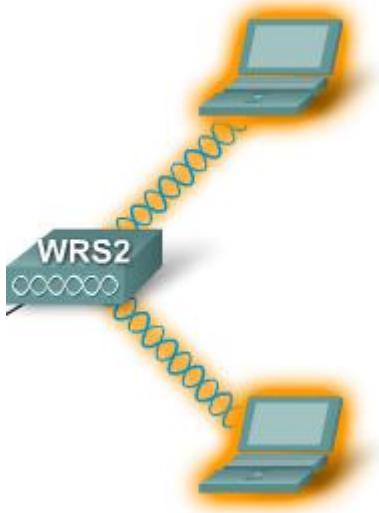


Composants d'un réseau local sans fil

- Périphériques LAN sans fil.
  - Dans un réseau local sans fil, chaque client utilise une carte réseau sans fil pour accéder au réseau via un périphérique sans fil tel qu'un routeur ou un point d'accès sans fil.

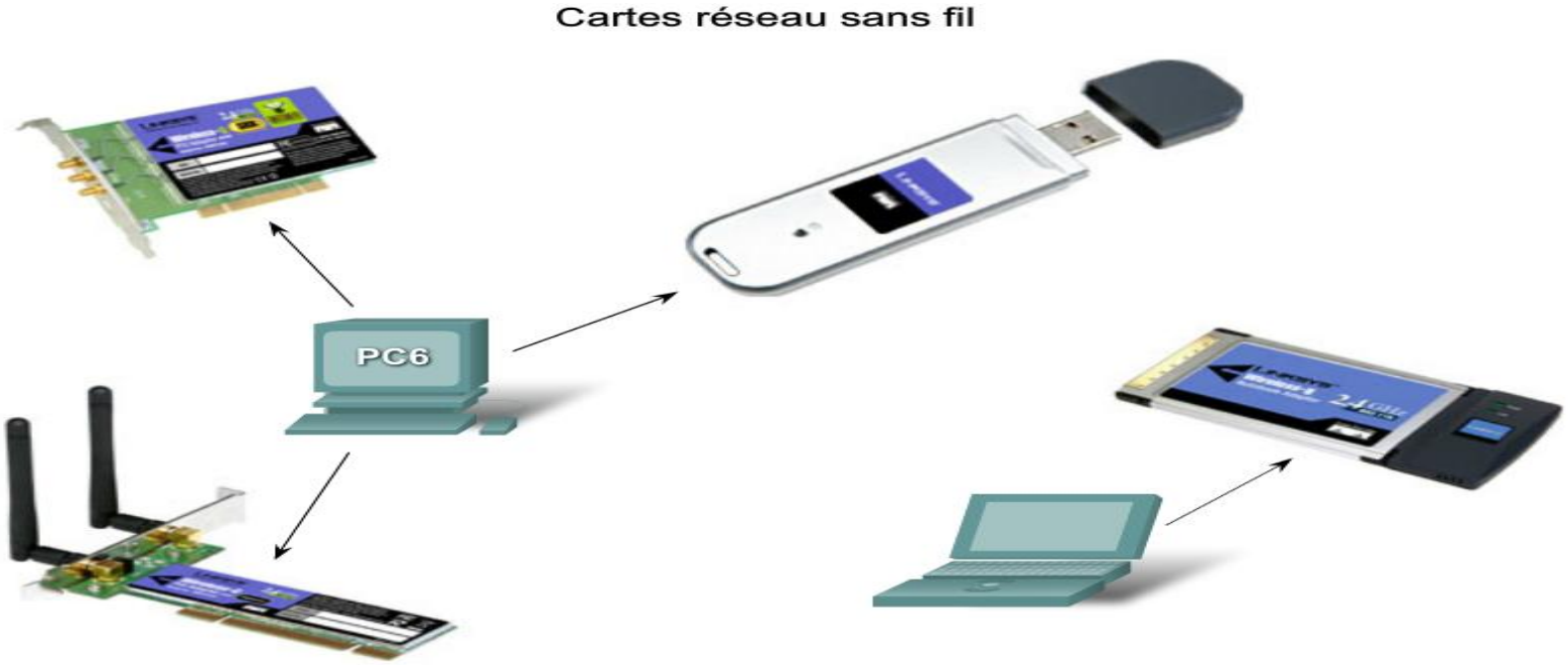


- Clients.
  - La carte réseau sans fil dont est équipé le client communique avec le routeur ou le point d'accès sans fil par le biais de signaux RF.



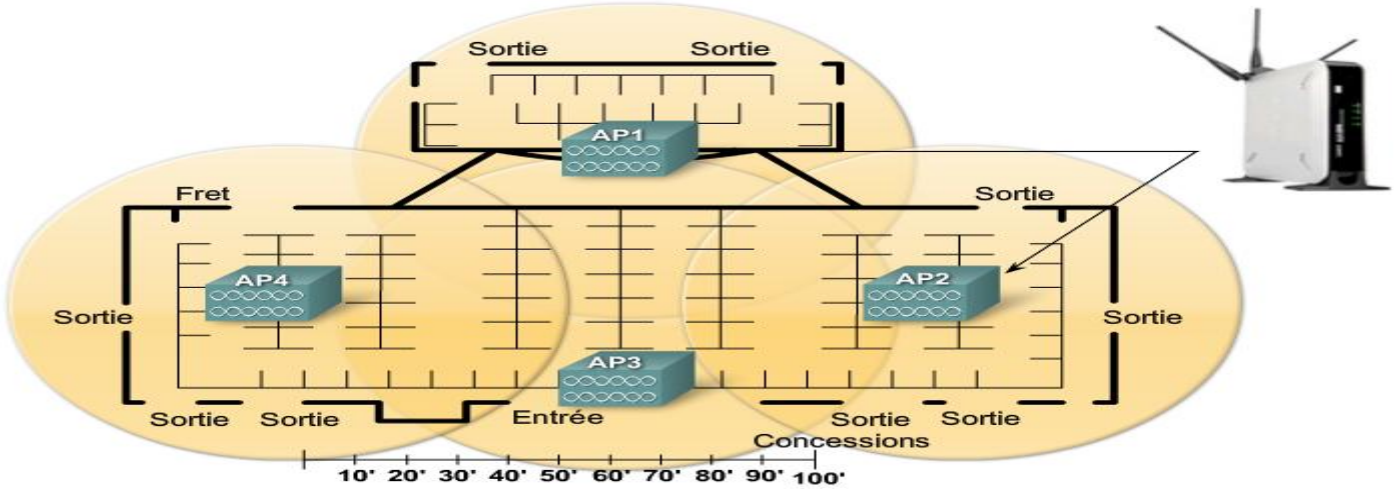
Composants d'une infrastructure sans fil

- Envoi et réception des signaux RF
  - Codage des flux sur un signal RF : Modulation
  - Comptabilité avec plusieurs normes (a/b/g/n)
  - Périphérique intégré ou extension



Composants d'une infrastructure sans fil

- **Points d'accès sans fil**
  - Un point d'accès permet de relier des clients sans fil (ou stations) à un réseau local filaire.
  - Conversion des paquets 802.11/802.3 (vice-versa)
    - Un point d'accès convertit les paquets de données TCP/IP, les faisant passer de leur format d'encapsulation de trames radio 802.11 au format de trame Ethernet 802.3 sur le réseau Ethernet filaire.
  - Périphérique de couche 2 ou couche 3 (Routeur sans fil)



Composants d'une infrastructure sans fil

- **Les Routeurs sans fil:** jouent le rôle de:
  - point d'accès qui assure les fonctions classiques d'un point d'accès,
  - commutateur Ethernet intégré 10/100 bidirectionnel simultané à quatre ports, qui fournit une connectivité aux périphériques filaires,
  - routeur qui procure une passerelle pour se connecter aux autres infrastructures réseau.

Composants d'une infrastructure sans fil

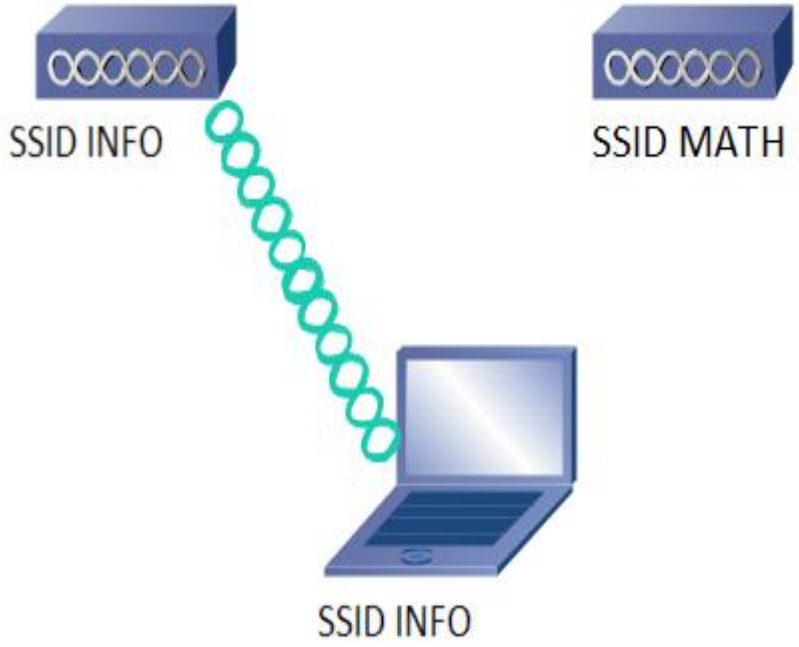
Dans les petites entreprises et chez les particuliers, les routeurs sans fil jouent le rôle de point d'accès, de commutateur Ethernet et de routeur.

Association du client au point d'accès

- Processus visant à établir une liaison de données entre un point d'accès et un client du réseau
- Les principales composantes de ce processus sont les suivantes :
  - **Trames Beacon** - Trames utilisées par le RLSF pour annoncer sa présence. (SSID, Débit, Sécurité)
  - **Analyseurs** - Trames utilisées par les clients des RLSF pour trouver leur réseau.
  - **Authentification** vérification de l'identité ou d'un processus
  - **Association** - Processus visant à établir une liaison de données entre un point d'accès et un client de RLSF.

Service Set IDentifier

- Permet de séparer logiquement les WLAN
  - Doit être le même sur le client et le point d'accès
- L'accès point diffuse un **SSID** par fréquence porteuse
- Association en 5 étapes
  - Requête du client
  - Service Set IDentifier
  - Réponse du point d'accès
  - Client initie l'association
  - Le point d'accès accepte l'association
    - Demande de clé de cryptage parfois
- Ajout de l'@MAC du client dans la table d'association Similaire ➡ à la commutation LAN



Fonctionnement sans fil

- Paramètres configurables pour les points d'extrémité sans fil
  - La figure présente l'écran initial de configuration sans fil d'un routeur sans fil Linksys.
  - Lorsqu'un point d'accès Linksys est configuré pour autoriser les clients 802.11b et 802.11g, il fonctionne en mode mixte.

Avantages

Avantages et limites de la technologie sans fil

- **Mobilité** : facilite la connexion des clients fixes et mobiles.
- **Évolutivité** : peut facilement être étendue afin d'autoriser d'autres utilisateurs à se connecter et d'augmenter la zone de couverture.
- **Souplesse** : offre une connectivité en tout lieu et à tout moment.
- **Économies** : le coût des équipements continue de baisser à mesure que la technologie progresse.
- **Temps d'installation réduit** : l'installation d'un seul équipement peut offrir une connectivité à un grand nombre de personnes.
- **Fiabilité dans des environnements difficiles** : facilité d'installation dans des environnements d'urgence et hostiles.

Inconvéniants

Limites de la technologie de réseau local sans fil

- **Interférence** : la technologie sans fil est susceptible de faire interférence avec d'autres appareils qui produisent de l'énergie électromagnétique, par exemple les téléphones sans fil, les fours à micro-ondes, les téléviseurs et d'autres installations de réseau local sans fil.
- **Sécurité du réseau et des données** : la technologie de réseau local sans fil est conçue pour fournir un accès aux données transmises, et non pour assurer la sécurité des données. De plus, elle peut offrir un accès non protégé au réseau câblé.
- **Technologie** : la technologie de réseau local sans fil continue d'évoluer. Elle ne propose pas pour le moment la vitesse ou la fiabilité des réseaux locaux câblés.

III. Déploiements des RLSF

Planification des RLSF

- La planification
  - Permet de spécifier le nombre et les positions où installer les points d'accès
- Les objectifs recherchés
  - Bonne couverture globale
  - Faible taux d'interférence
  - Débit élevé
- Paramètres à prendre en compte
  - Nombre de point d'accès à installer
  - Nombre d'utilisateurs
  - Structure géographique du bâtiment (Obstacles)

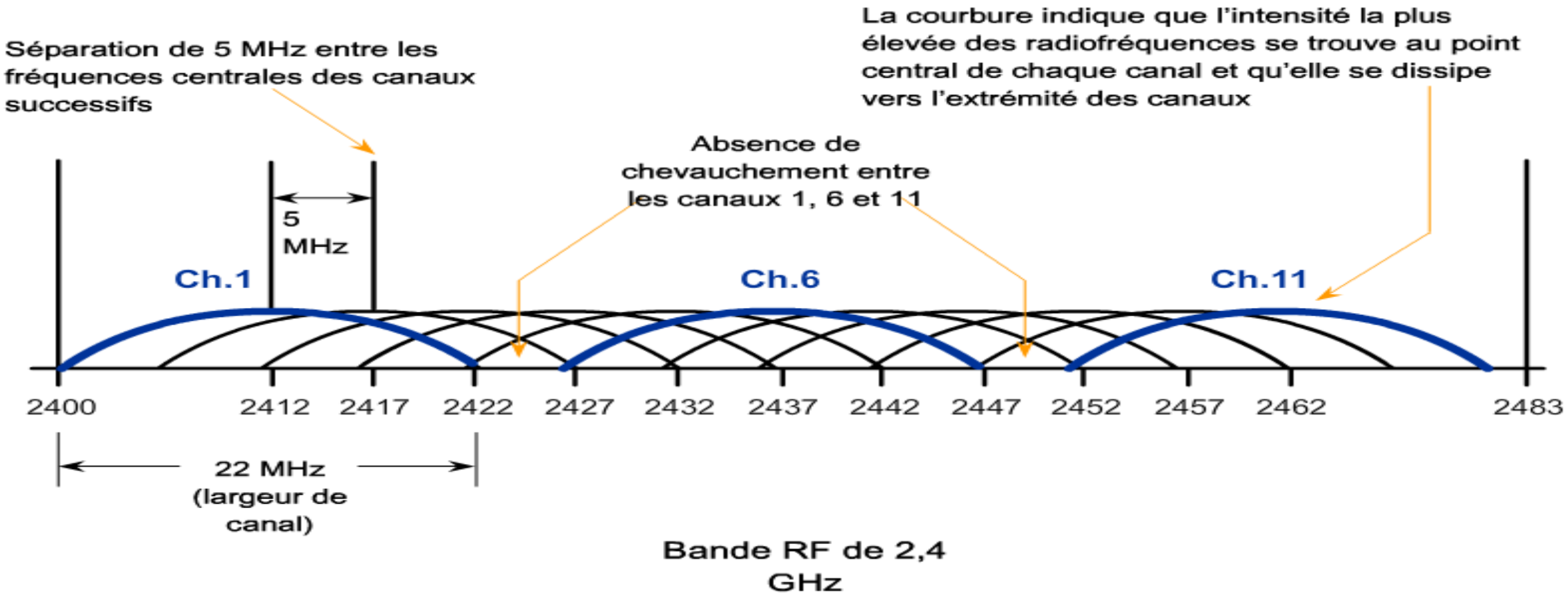
Planification des RLSF

Vue d'ensemble de la configuration du point d'accès sans fil

- Étape 1 : vérifiez le fonctionnement du réseau local filaire, DHCP et accès Internet
- Étape 2 : installez le point d'accès
- Étape 3 : configurez le point d'accès, SSID, (pas encore de dispositif de sécurité)
- Étape 4 : installez un client sans fil (pas encore de dispositif de sécurité)
- Étape 5 : vérifiez le fonctionnement du réseau sans fil
- Étape 6 : configurez la sécurité sans fil, WPA2 avec PSK
- Étape 7 : vérifiez le fonctionnement du réseau sans fil

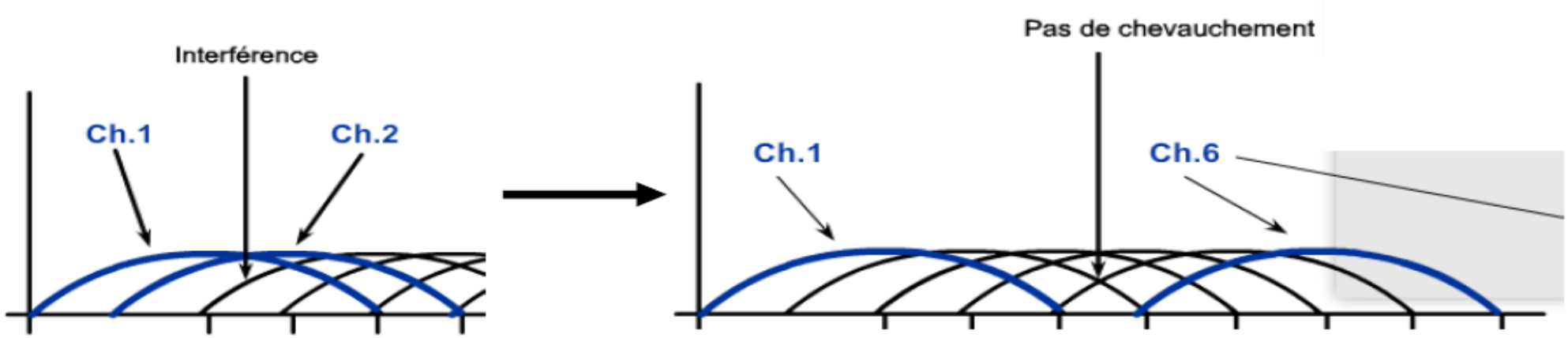
Les Fréquences

- Type de réseaux sans fil : 802.11 a/b/g ou n
- Les canaux (interférences des canaux adjacents)



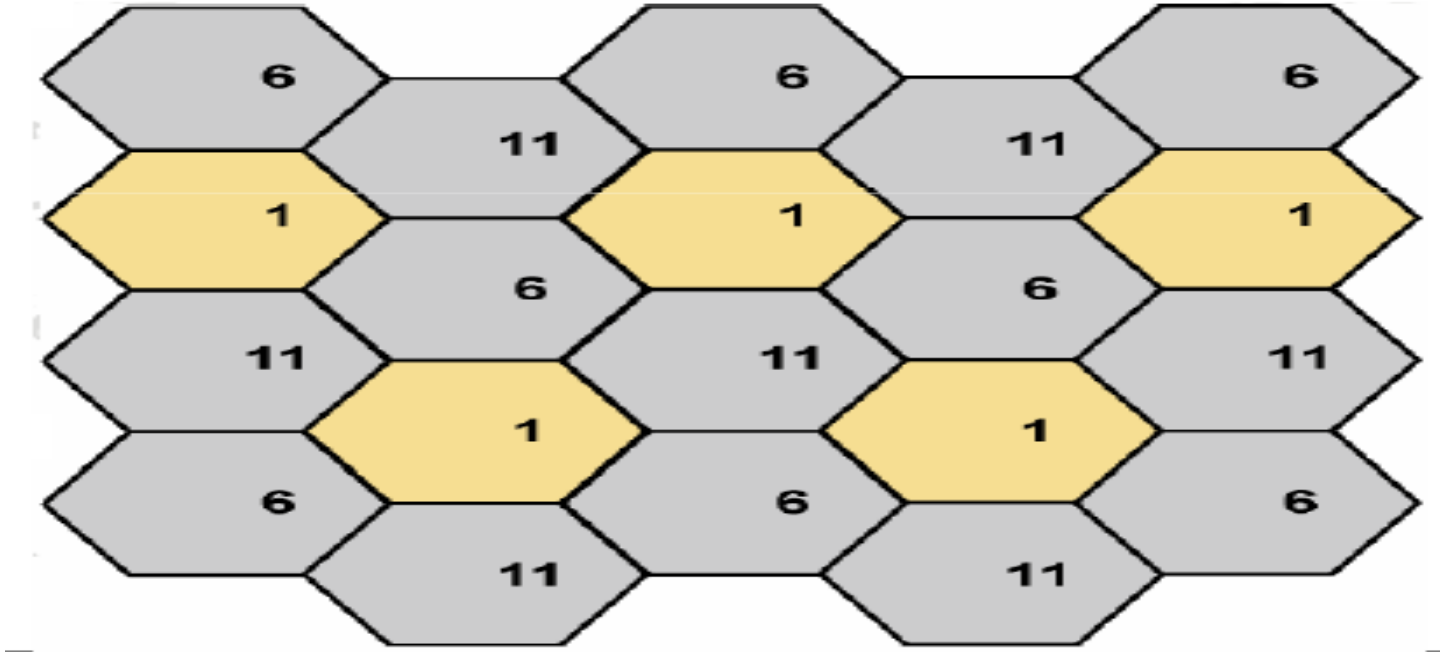
Interférences des canaux

- Interférences
  - Chevauchement des canaux adjacents
- Conséquences
  - Connectivité instable ou même inexistante
- Éloigner les canaux des points d'accès voisins
  - Utiliser des canaux non interférents



Planification du réseau local sans fil

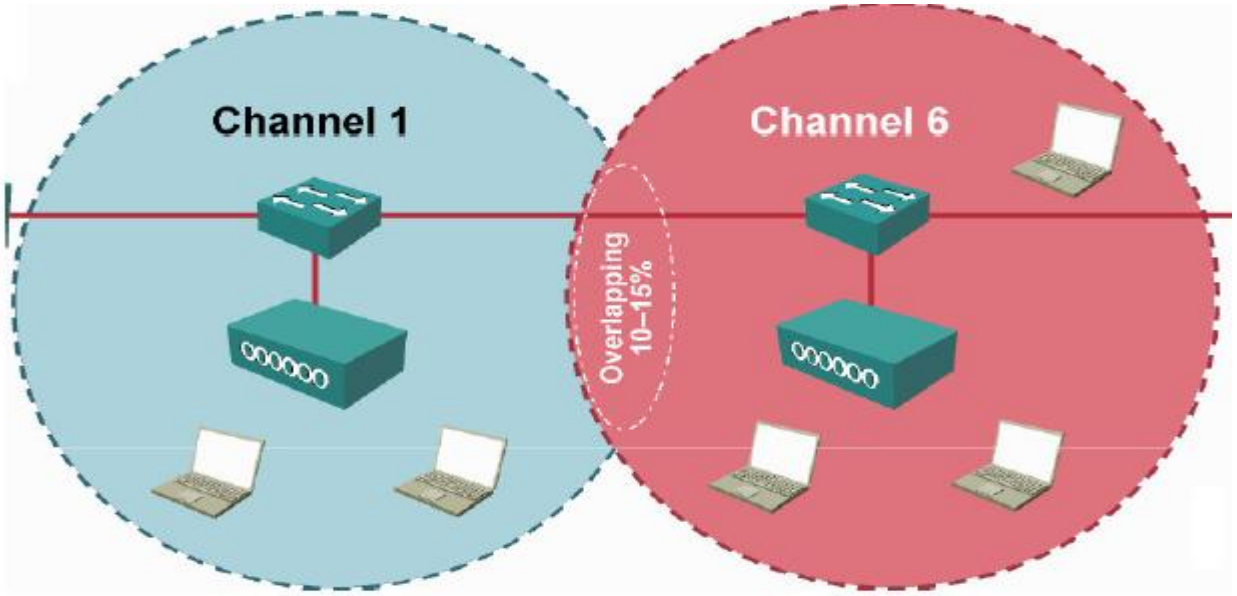
- Placement optimal des AP afin d'éviter les interférences de canaux voisins
  - Réutilisation des canaux non interférents



Planification du réseau local sans fil

❑ Recouvrement

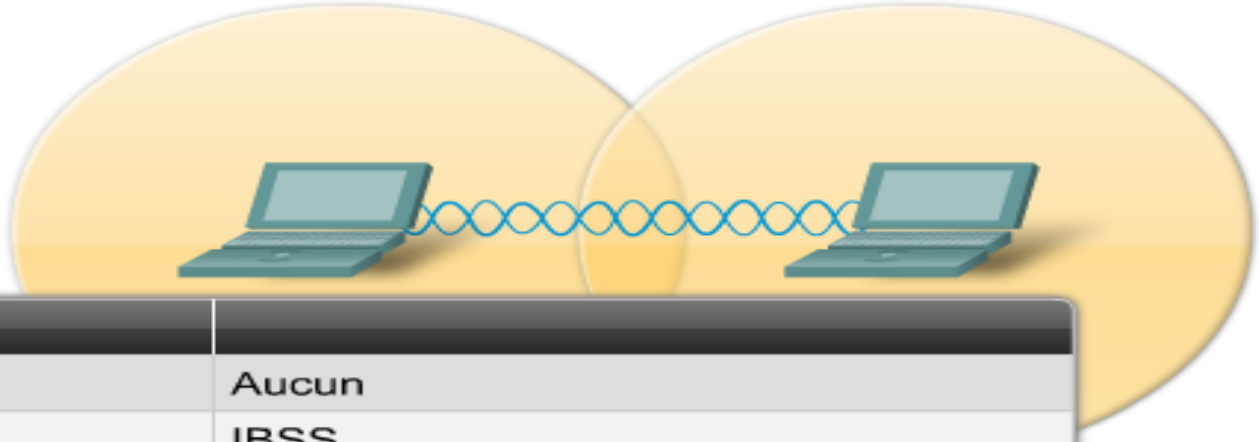
- Si l'AP1 est sur le canal 1
  - Les autres AP doivent être sur les canaux 6 ou plus pour ne pas provoquer de zones d'interférence
- Planification radio



Les différents types de topologies 802.11

Réseaux ad hoc

- peuvent fonctionner sans points d'accès
- Les stations client configurées pour fonctionner en mode **ad hoc** se configurent entre elles les paramètres sans fil.
- La norme IEEE 802.11 désigne un réseau **ad hoc** sous le nom **IBSS** (Independent basic service set), ensemble de services de base indépendant).



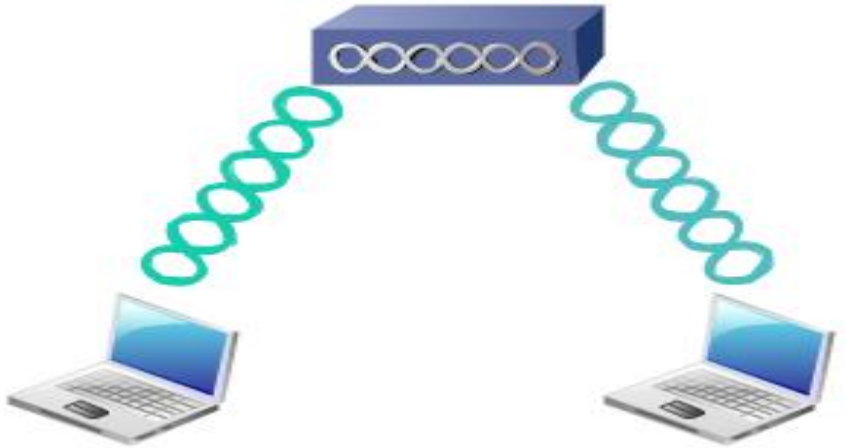
Points d'accès	Aucun
Diagramme de topologie	IBSS
Connexion	Peer to peer
Mode	Ad hoc
Couverture	Zone de service de base (BSA)

Les différents types de topologies 802.11

Ensembles de services de base

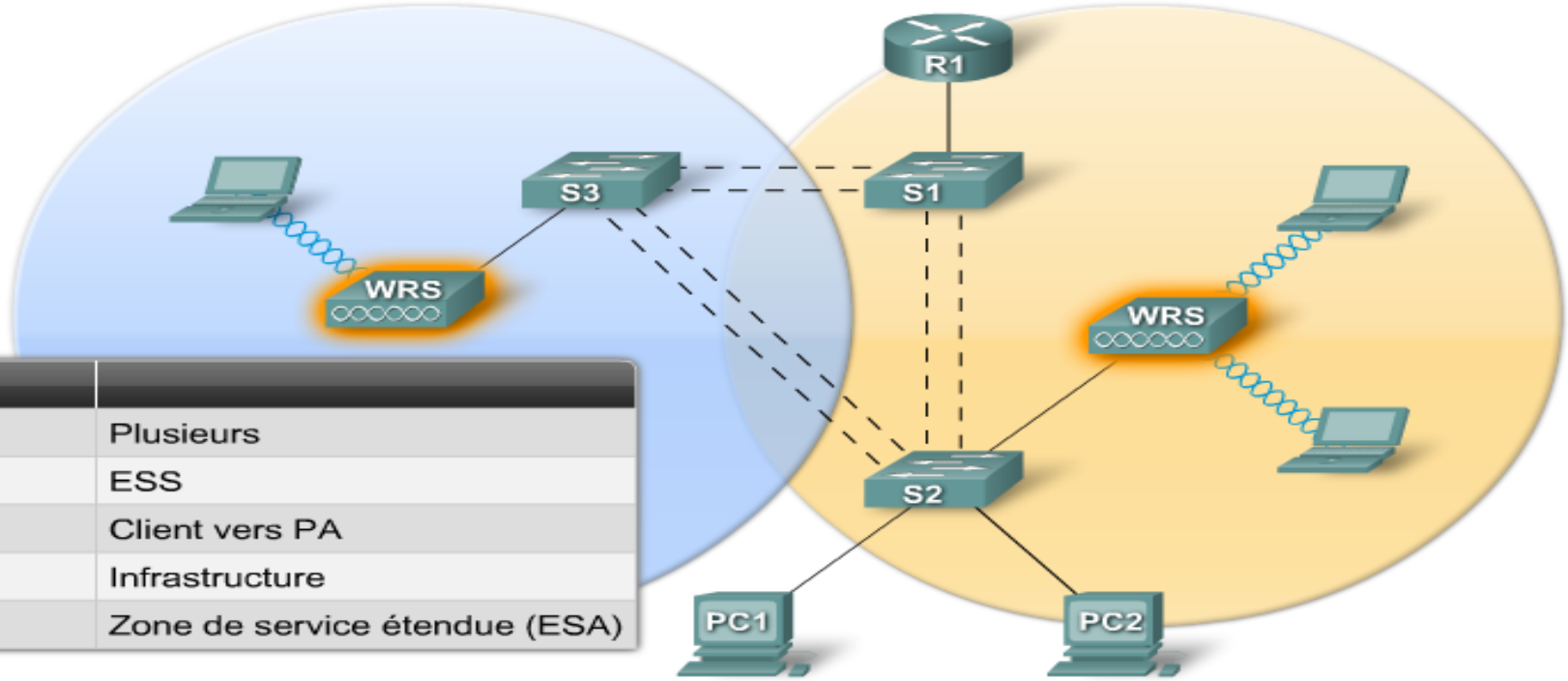
- Les points d'accès améliore la portée des clients.
- Un seul point d'accès en mode infrastructure permet de gérer les paramètres sans fil et la topologie consiste simplement en un ensemble de services de base.
- La zone de couverture d'un **IBSS** et d'un **BSS** est **BSA** appelée (basic service area) ou microcellule.

Points d'accès	Un
Diagramme de topologie	BSS
Connexion	Client vers PA
Mode	Infrastructure
Couverture	Zone de service de base (BSA)



Les différents types de topologies 802.11

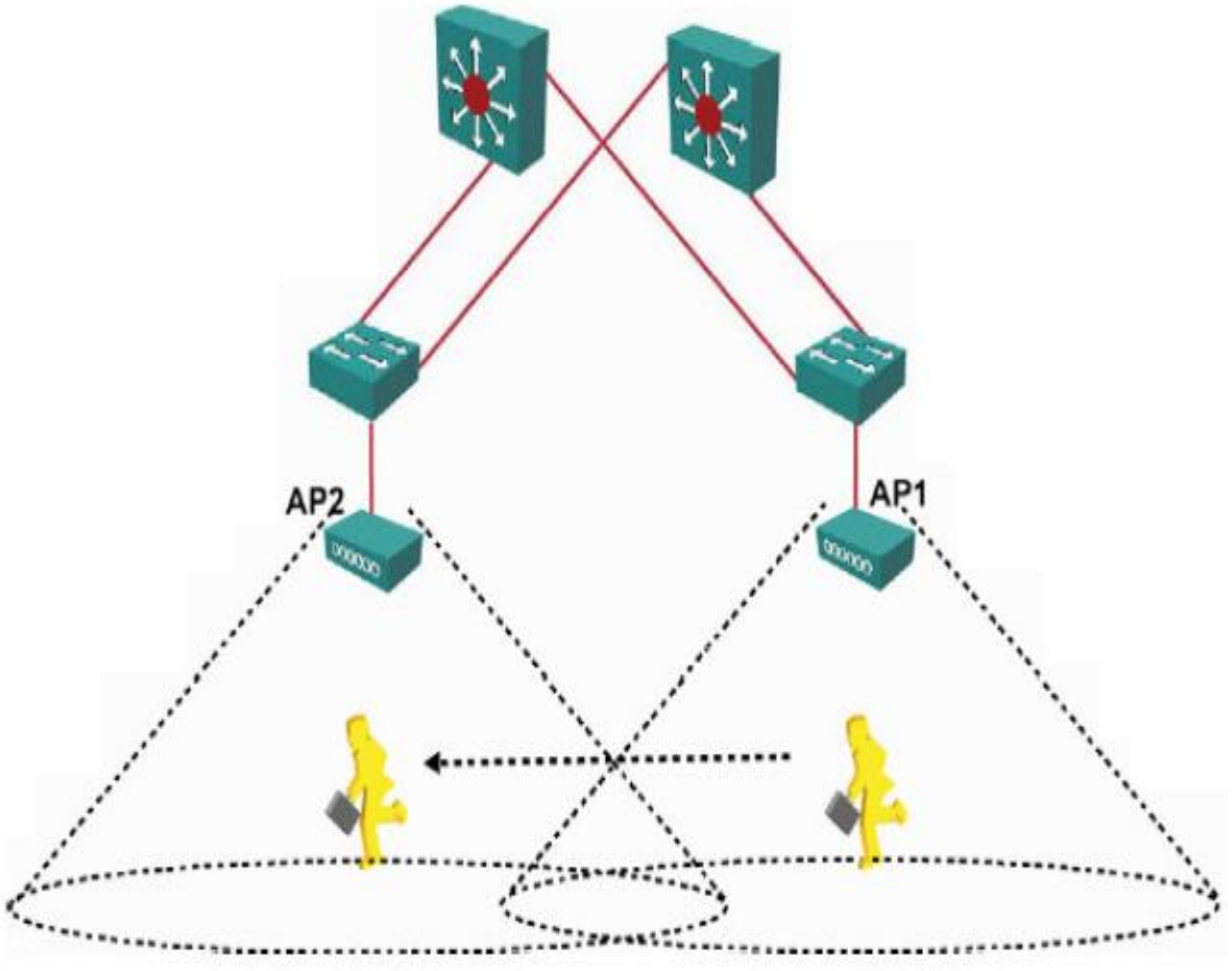
- **ESS** (extended service set). **Éventails de services étendus**
  - Plusieurs **AP** qui crée un WLAN. Zone de couverture plus grande et possibilité de roaming,
  - Dans un **ESS**, un **BSS** se distingue d'un autre par son identificateur (**BSSID**), qui correspond à l'adresse MAC du point d'accès desservant le **BSS**.
  - **ESA** (Extended Service Area.).



Points d'accès	Plusieurs
Diagramme de topologie	ESS
Connexion	Client vers PA
Mode	Infrastructure
Couverture	Zone de service étendue (ESA)

Roaming

- Utilisateurs mobiles
  - Se déplace d'une AP vers une autre
  - Perte de connexion temporaire
  - Pour ne pas avoir de déconnexion
- Utiliser les mêmes SSID sur toutes les AP

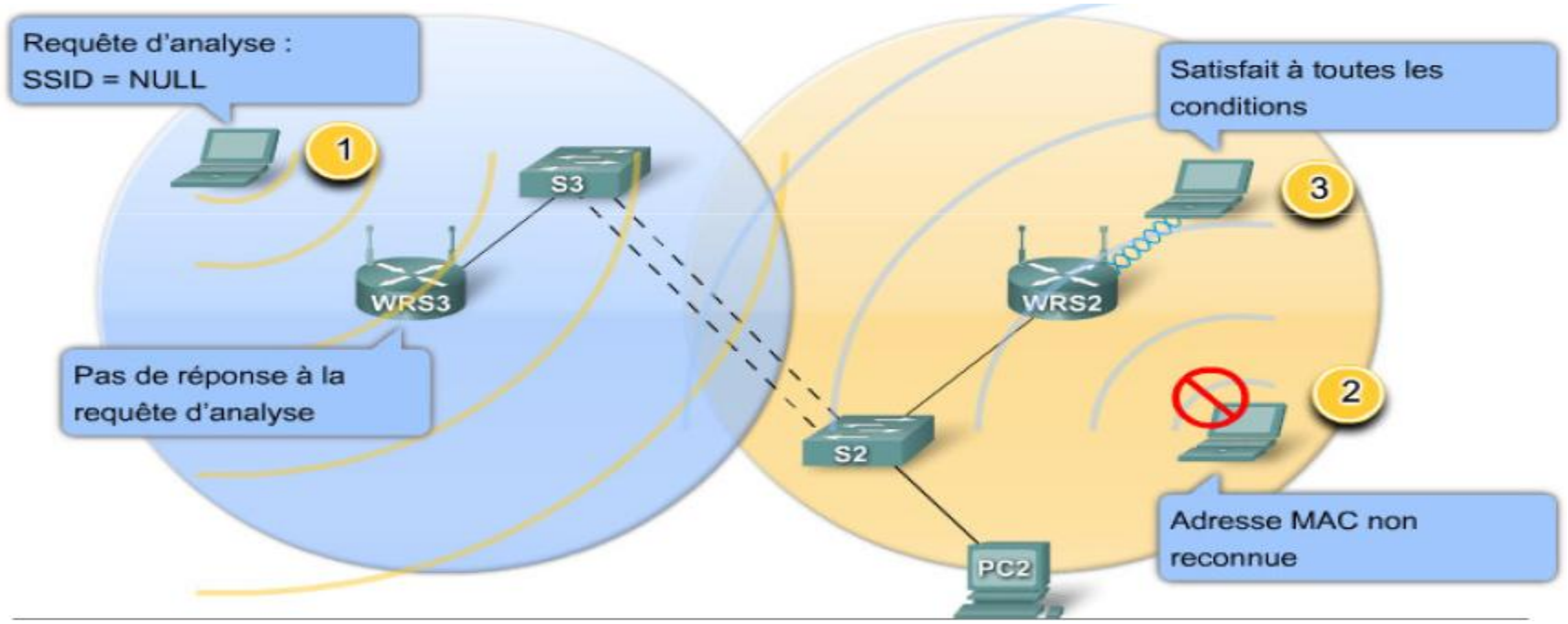


IV. Sécurité des réseaux locaux sans fil

Menaces de sécurité sur les RLSF

Sécurité : contrôle d'accès

- SSID non diffusé (Sécurité faible)
- Filtrage des adresses MAC (Sécurité faible)



Sécurité avancée

Vue d'ensemble des protocoles sans fil

Principales étapes de sécurisation des réseaux locaux sans fil

Accès ouvert	Chiffrement de première génération	Provisoire	Présent
SSID	WEP	WPA	802.11i/WPA2
• Aucun chiffrement • Authentification de base • N'est pas un dispositif de sécurité	• Authentification non efficace • Clés statiques, cassables • Non évolutif	• Standardisé • Chiffrement amélioré • Authentification utilisateur efficace (p.ex., LEAP, PEAP, EAP-FAST)	• Chiffrement AES • Authentification : 802.1X • Gestion des clés dynamiques • WPA2 correspond à la mise en œuvre de la norme 802.11i par la Wi-Fi Alliance

Sécurité avancée

- Paramètres de sécurité à contrôler
  - Authentification, Chiffrement, Intrusion
- WEP (Wired Equivalent Privacy) 1997
  - Clé statique variant de 64 à 128 bits configurée sur les clients et l'AP
  - Facilement cassable, pas d'authentification
- WPA (Wi-Fi Protected Access) 2003
  - Chiffrement plus avancé
- WPA2 2004
  - Cryptage AES, Gestion dynamique des clés
- WPA 2 Entreprise (Radius)
  - Authentification IEEE 802.1X

Sécurité : Authentification

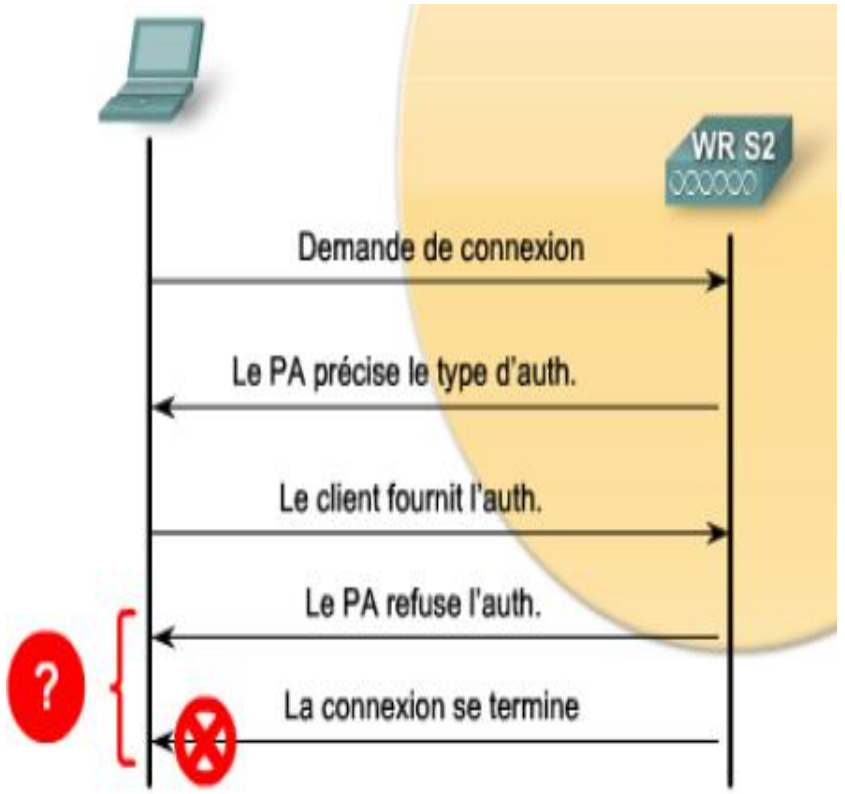
Processus de sécurité

- Activer le chiffrement WEP ou WPA, WPA2 (AES)
- Authentification IEEE 802.1X (Serveur AAA)
- Pour les entreprises, WPA2 inclut une connexion à une base de données RADIUS (Remote Authentication Dial In User Service).

Chiffrement

- Le même algorithme de chiffrement doit être utilisé entre le serveur et le client

  - WEP ⟹ Chiffrement WEP
  - WPA ⟹ Chiffrement TKIP
  - WPA2 ⟹ Chiffrement AES



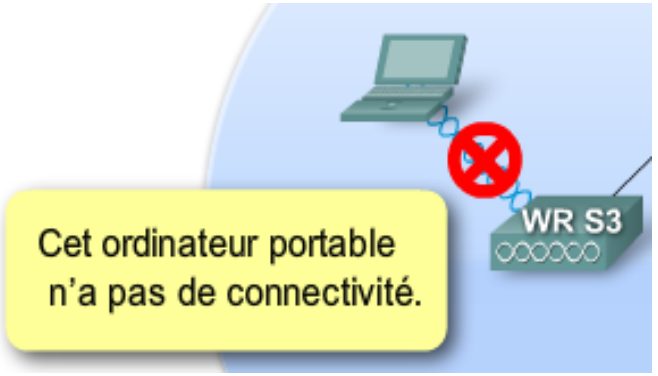
Chiffrement

TKIP – Temporal Key Integrity Key	AES – Advanced Encryption Standard
• Chiffrement par l'ajout de codage de bits de plus en plus complexe à chaque paquet • Basé sur le même algorithme de chiffrement (RC4) que WEP	• Nouvel algorithme de chiffrement utilisé dans 802.11i • Basé sur TKIP avec des fonctionnalités supplémentaires qui améliorent le niveau de sécurité offert

V. Dépannage des RLSF

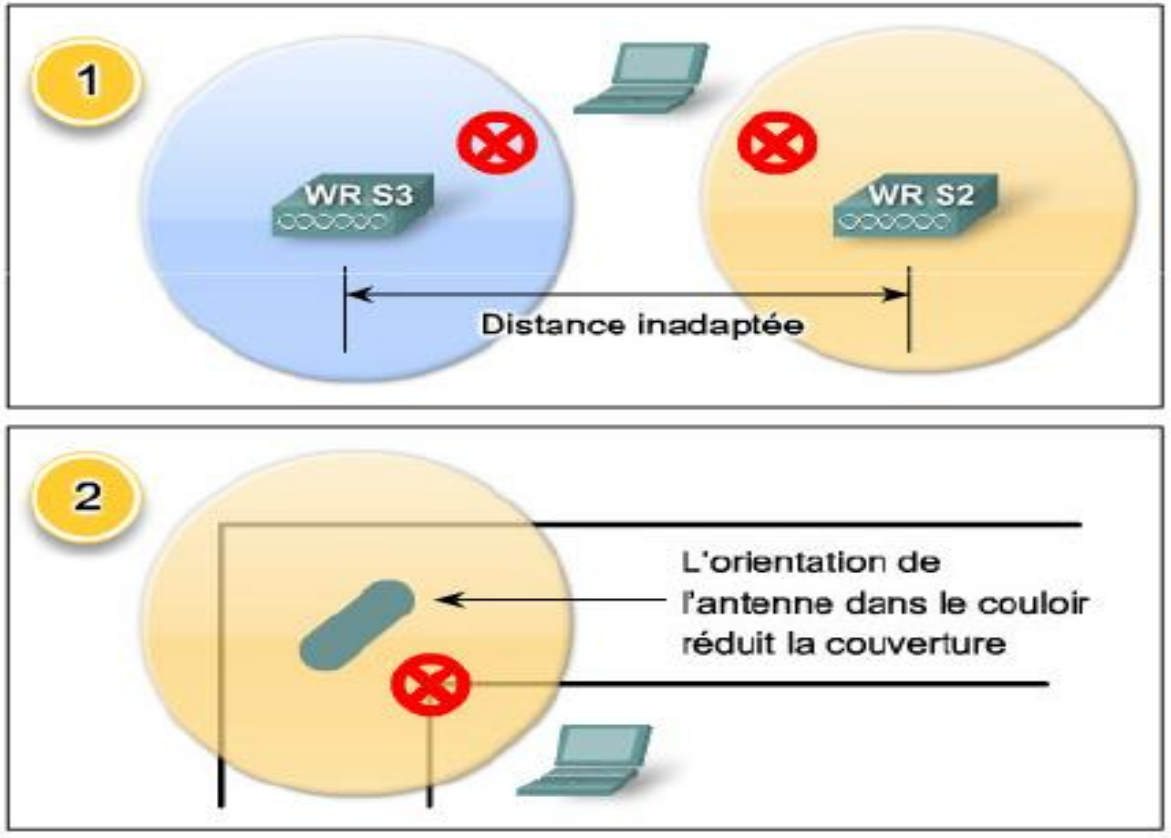
Dépannage des RLSF

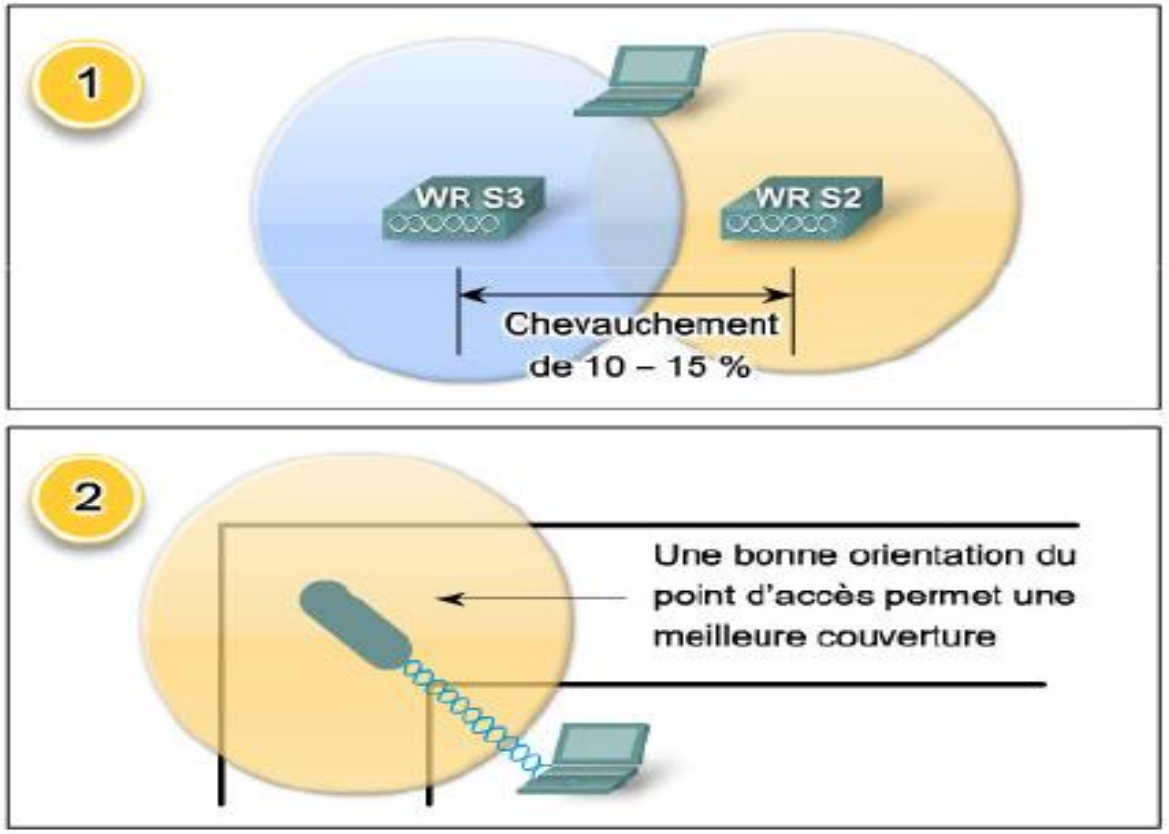
- Procédure étape par étape afin de dépanner des problèmes de connexion à un RLSF
  - Vérifier les paramètres IP du PC
  - Vérifier que le PC peut se connecter au réseau filaire
  - Vérifier la carte réseau sans fil (pilote logiciels) ou même changer la carte
  - Vérifier que vous avez entré les bons paramètres de sécurité
    - Clé WEP ou WPA
    - Authentification RADIUS



Autres problèmes

- ✓Éloignement des points d'accès sans fil
- ✓ Orientation des antennes





Conclusion

- Avec les débits actuels
  - Applications voix sur les WLAN
  - Sécurité un point important à prendre en compte
- Chiffrement WEP et évolution vers WPA2
  - Authentification (RADIUS)
- La norme 802.11n est actuellement fonctionnelle
  - Débit théorique de 300Mb/s
- Réseaux locaux sans fil de plus en plus présent dans le futur
  - Hot spots, Routeur ADSL etc…