WLAN : les réseaux sans fils et WiFi

Camille Diou

Docteur en microélectronique

LABORATOIRE INTERFACES CAPTEURS & MICROÉLECTRONIQUE

UNIVERSITÉ DE METZ

WLAN : les réseaux sans fils et WiFi

- Introduction
- Les réseaux IEEE 802.11x
- Architecture WiFi
- Fonctionnalités
- La sécurité
- Les trames
- Configuration et installation

INTRODUCTION

Introduction

- 1990 : groupe IEEE 802.11
- 1997 : standard IEEE 802.11
- 1 couche MAC, 3 couches physiques :
  - FHSS : Frequency Hopping Spread Spectrum — 802.11b
  - DSSS : Direct Sequence Spred Spectrum — 802.11b
  - IR : InfraRed — 802.11b
  - OFDM : Orthogonal Frequency Division Multiplexing — 802.11g

  Bande ISM
  - produits incompatibles mais interopérables via la LLC
- Norme d'interopérabilité :
  - WiFi (Wireless Fidelity) délivré par le WECA (Wireless Ethernet Compatibility Alliance) pour IEEE 802.11b
  - WiFi-5 : IEEE 802.11a

Introduction

IEEE 802.11 : normalisation des WLAN

Norme d'interopérabilité du WECA

Technologie Apple

Les réseaux IEEE 802.11b

Wi Fi Architecture

Wi Fi architecture cellulaire

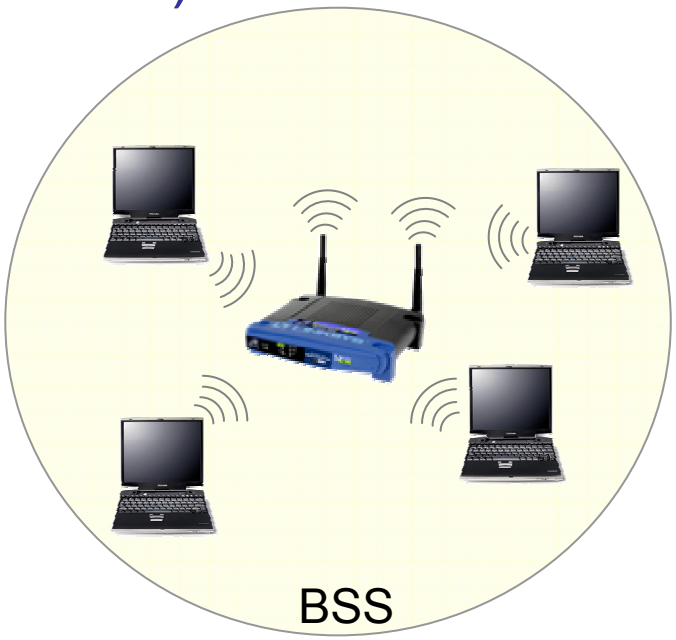
- similaire à la téléphonie mobile : téléphones + stations
- un ou plusieurs points d'accès : unifier le réseau et servir de pont
- → cellule

Wi Fi deux types de topologies

- mode infra-structure
  - BSS : Basic Service Set
  - ESS : Extended Service Set
- mode ad-hoc
  - IBSS Independent Basic Service Set

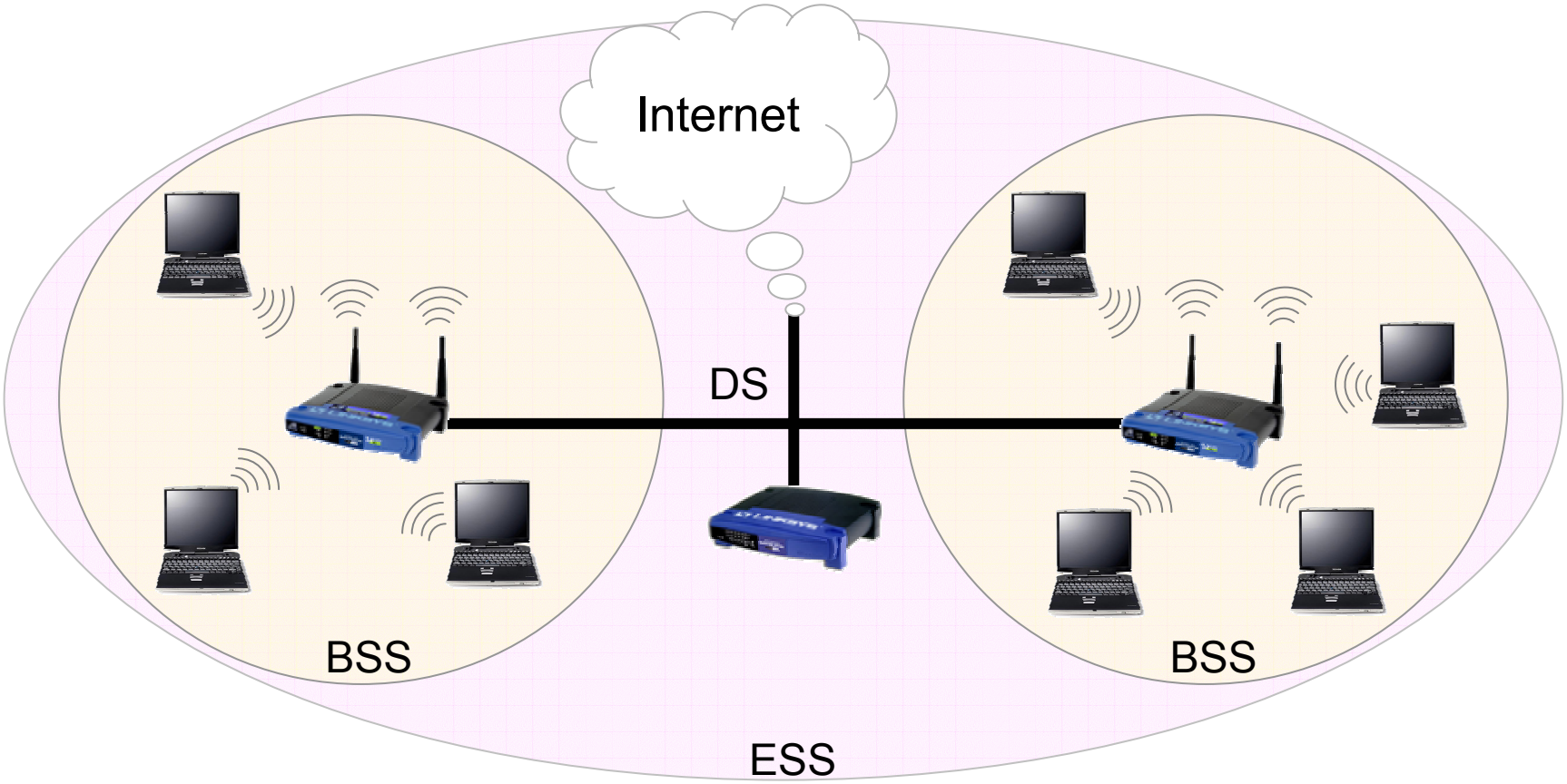
Le mode infra-structure : BSS

- Le mode infrastructure désigne un réseau composé d'une infrastructure permettant l'échange d'information entre les stations ; l'infrastructure est le point d'accès
- 1 cellule = 1Basic Service Set (BSS) = 1 point d'accès
- 100 stations : support partagé entre toutes les stations, ainsi que le débit (11 Mbits/s)



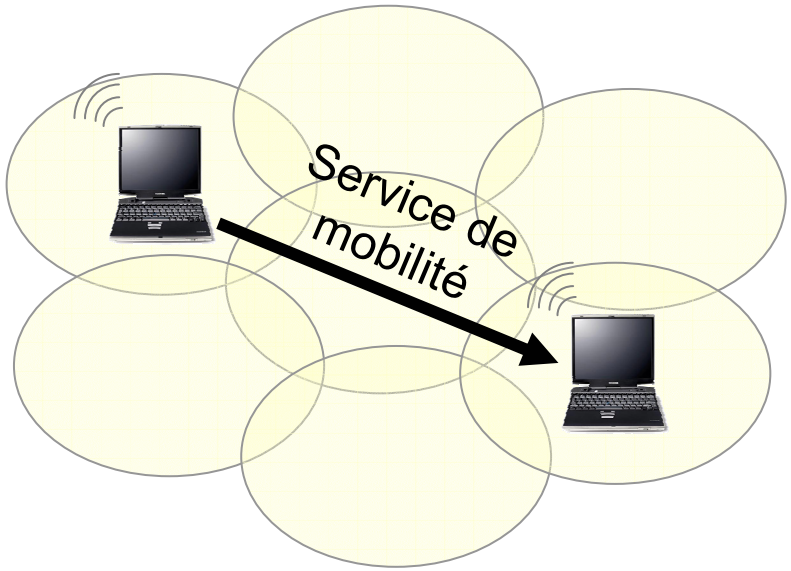
Le mode infra-structure : ESS

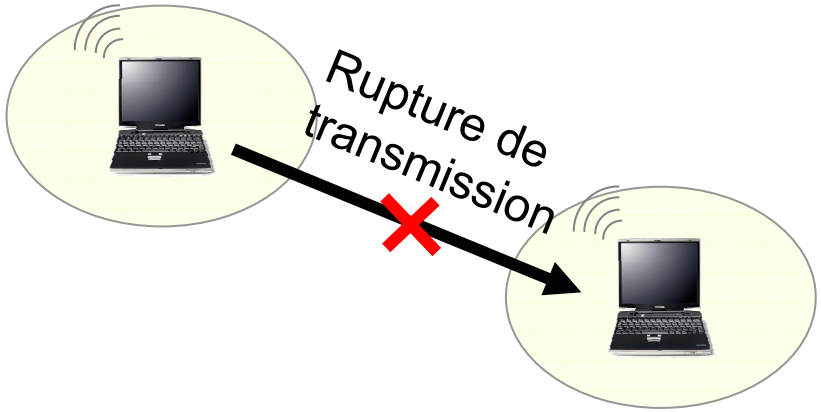
- Extended Service Set : plusieurs points d'accès (BSS) connectés entre eux par un système de distribution (DS)
- DS : Ethernet ou un autre réseau WLAN
- Fourniture d'accès vers un autre réseau : Internet



Le mode infra-structure : ESS

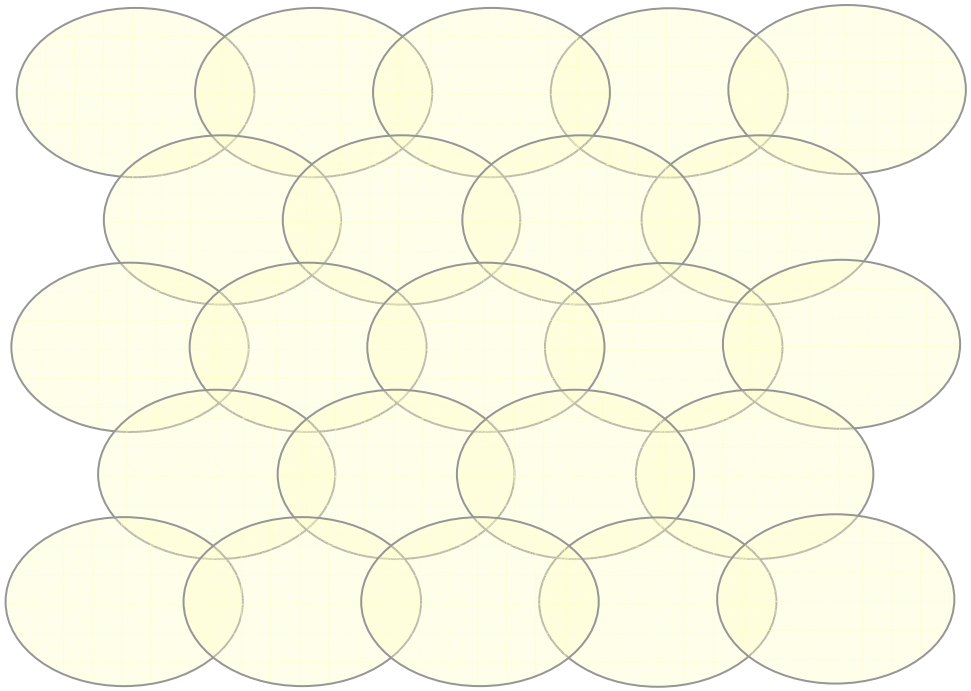
- Topologie ESS variable : cellules recouvrantes ou non
- les cellules recouvrantes permettent d'offrir service de mobilité (IEEE 802.11f) : pas de pertes de connexions
- plus grand nombre d'utilisateurs possibles sans dégradation trop importante des performances





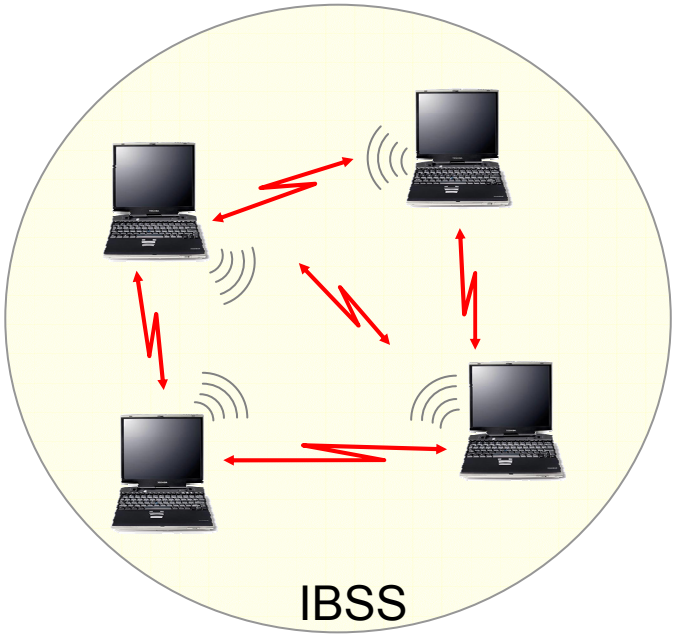
Réseau ambiant

- 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.)



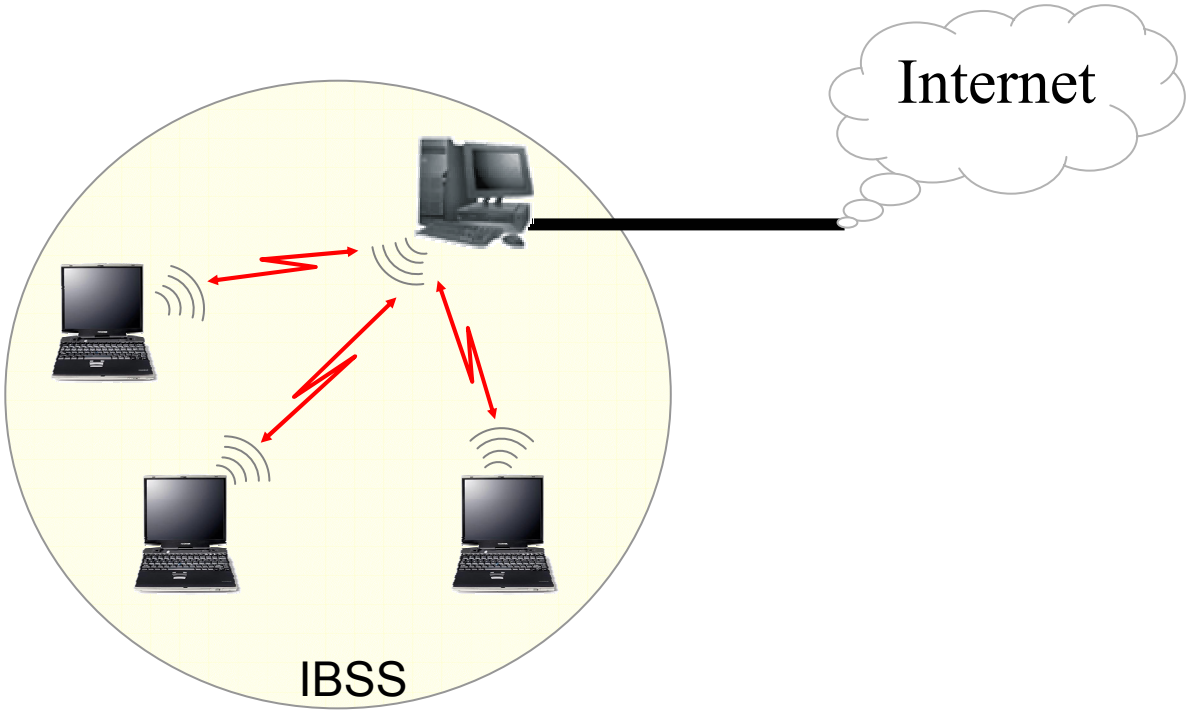
Le mode ad-hoc : IBSS

- Independent Basic Service Set : mode point à point
- Permet l'échange d'informations lorsque aucun point d'accès n'est disponible



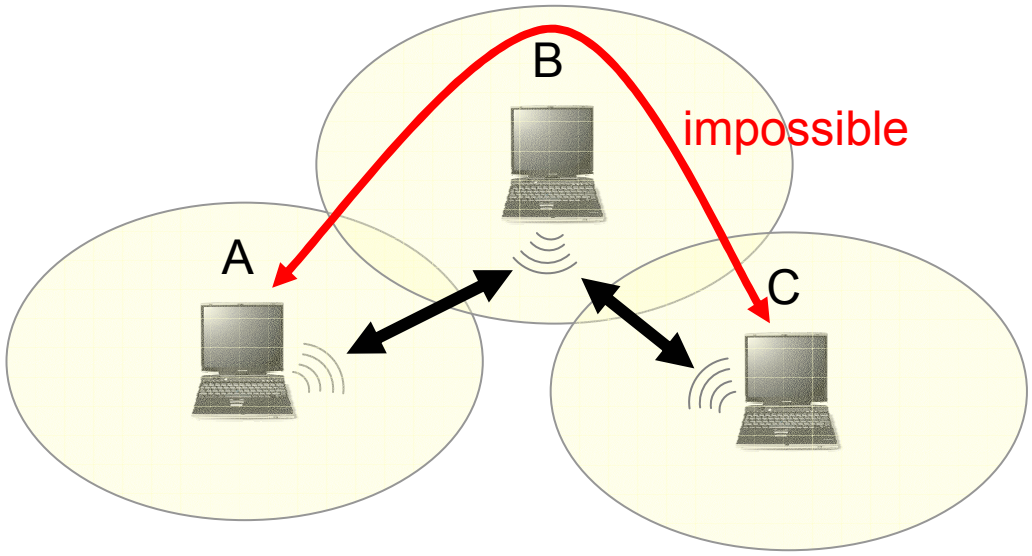
Le mode ad-hoc

- une station peut partager un accès à Internet : le réseau fonctionne comme un BSS



Le mode ad-hoc

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



3 stations en mode ad-hoc

Réseaux ad-hoc et routage

- Le logiciel de routage doit être présent dans 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

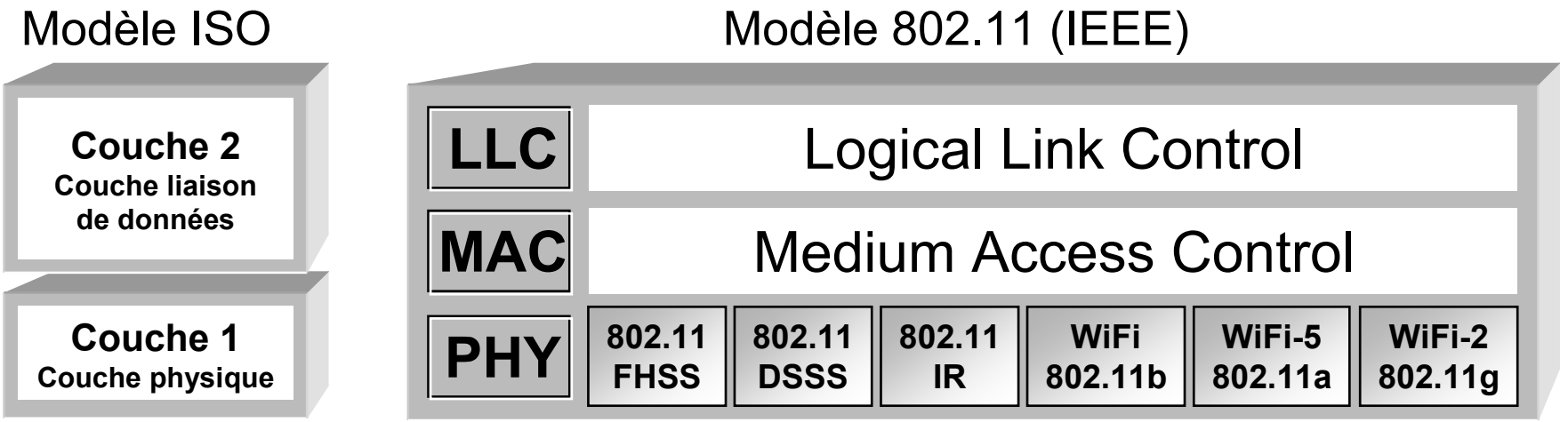
- Travaillent par inondation : détermination de la meilleure route lorsque les paquets sont prêts à être émis
- Pas d'échange de paquets de contrôle, sauf paquets de supervision (détermination du chemin)
- Le paquet de supervision diffusé vers les nœuds voisins est transmis par ceux-ci vers le nœud destination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

Protocoles proactifs

- Émission 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

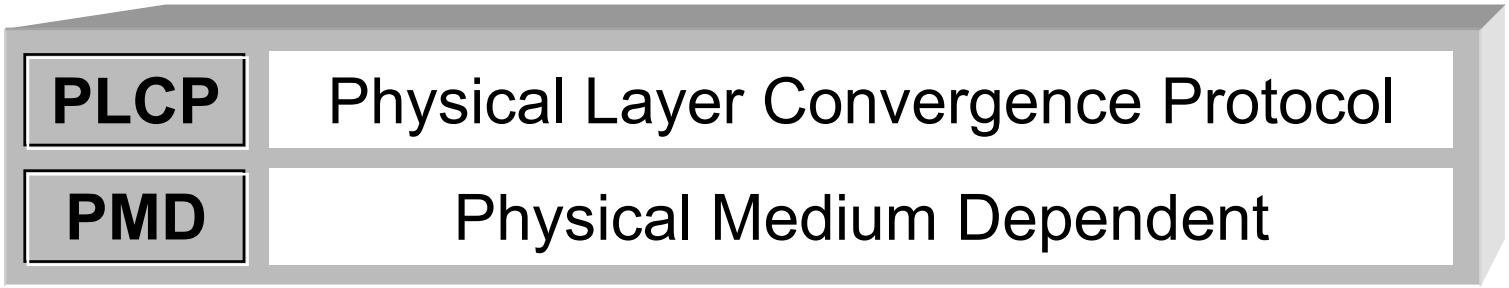
Architecture des systèmes IEEE 802.11x

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

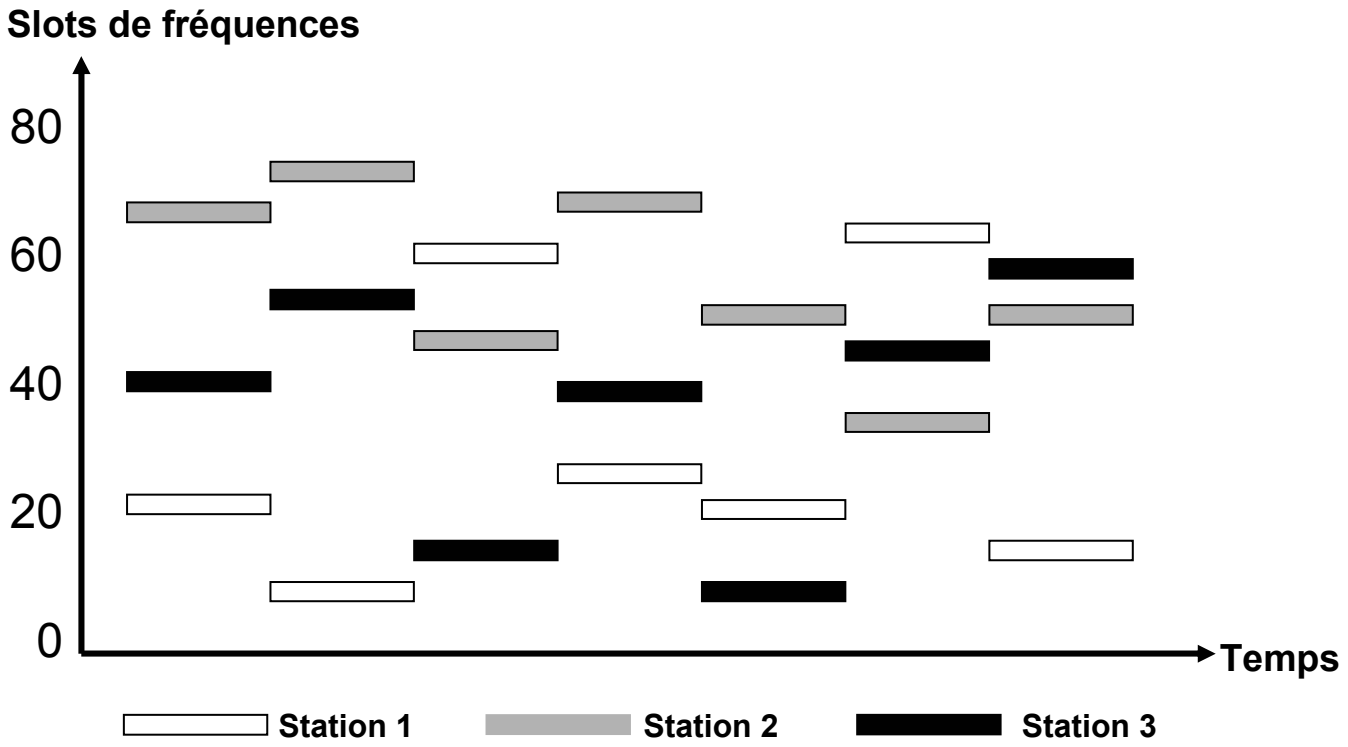


- Composée de deux sous-couches :
  - PMD gère l'encodage des données et de la modulation
  - PLCP gère l'écoute du support et signal à la couche MAC que le support est libre par un CCA (Clear Channel Assessment)

FHSS

Frequency Hopping Spread Spectrum

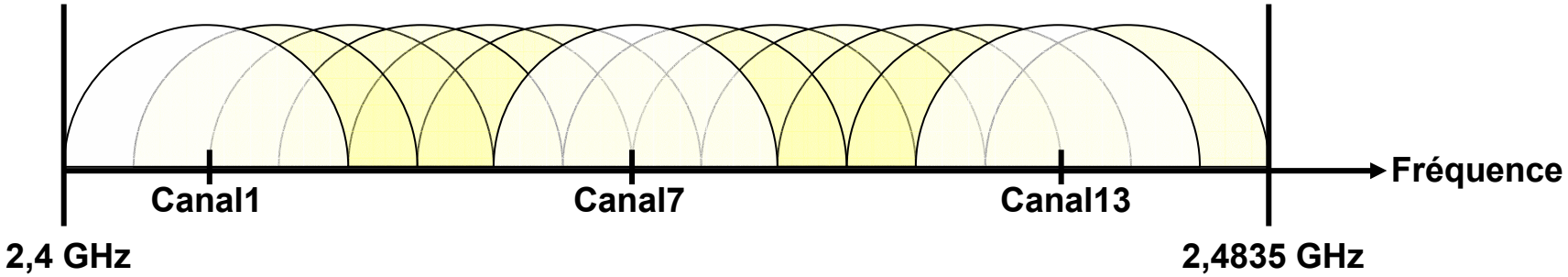
- 79 canaux de 1 MHz de largeur de bande
- 3 ensembles de 26 séquences, soit 78 séquences de sauts possibles
- Exemple : 3 stations sur 7 intervalles de temps : émission simultanée mais pas sur le même canal



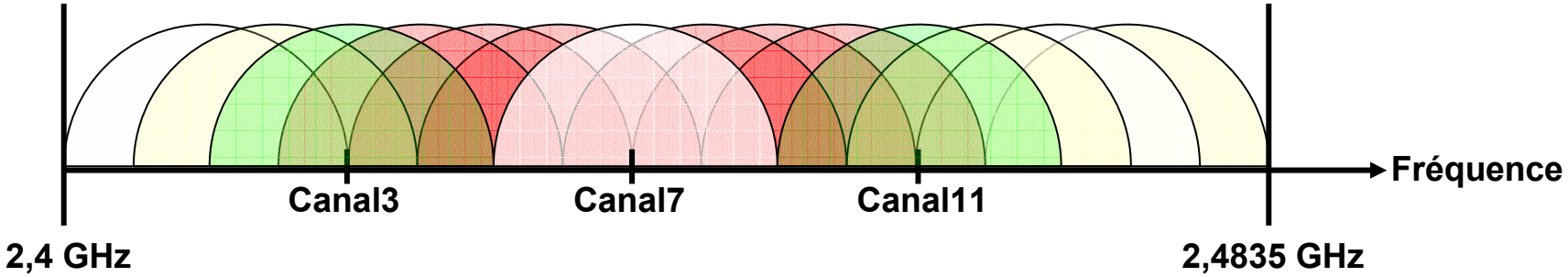
DSSS

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



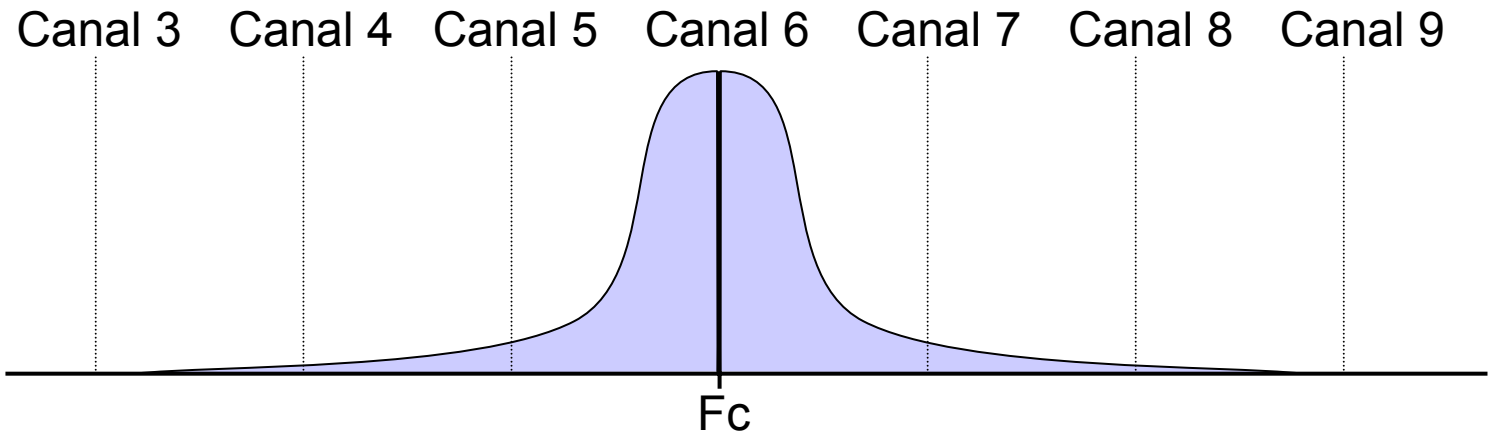
- Largeur totale de la bande = 83,5 MHz
- Canaux recouvrant : inexploitables simultanément



WiFi 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



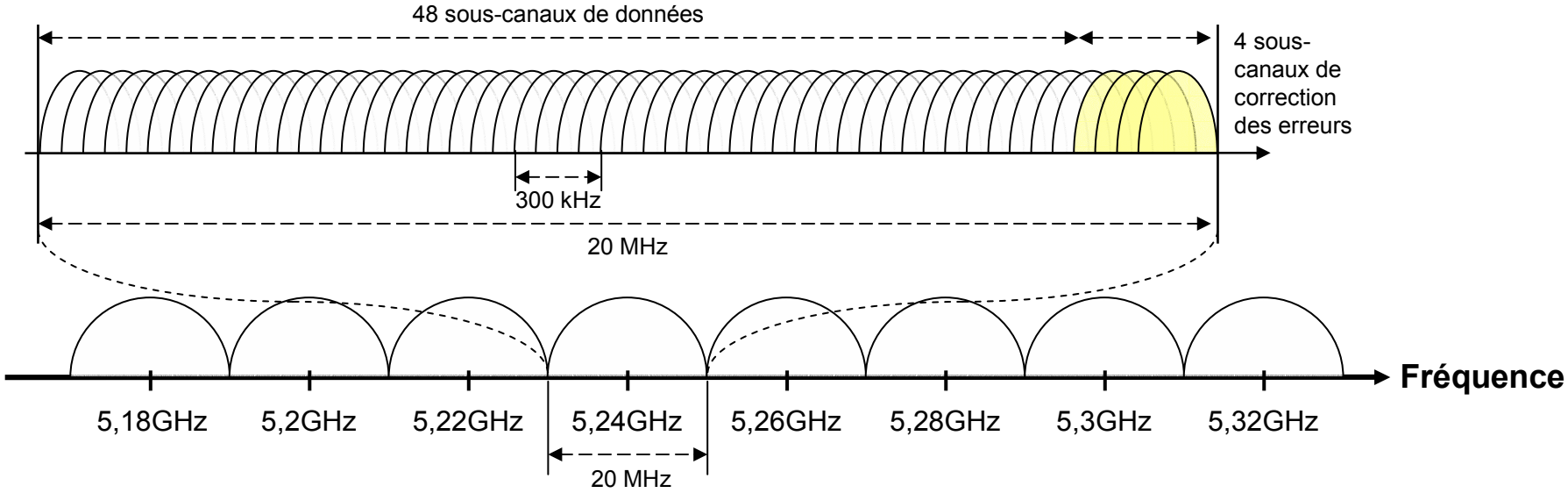
Spectre d'un canal

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

Wi Fi 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



La couche liaison de données

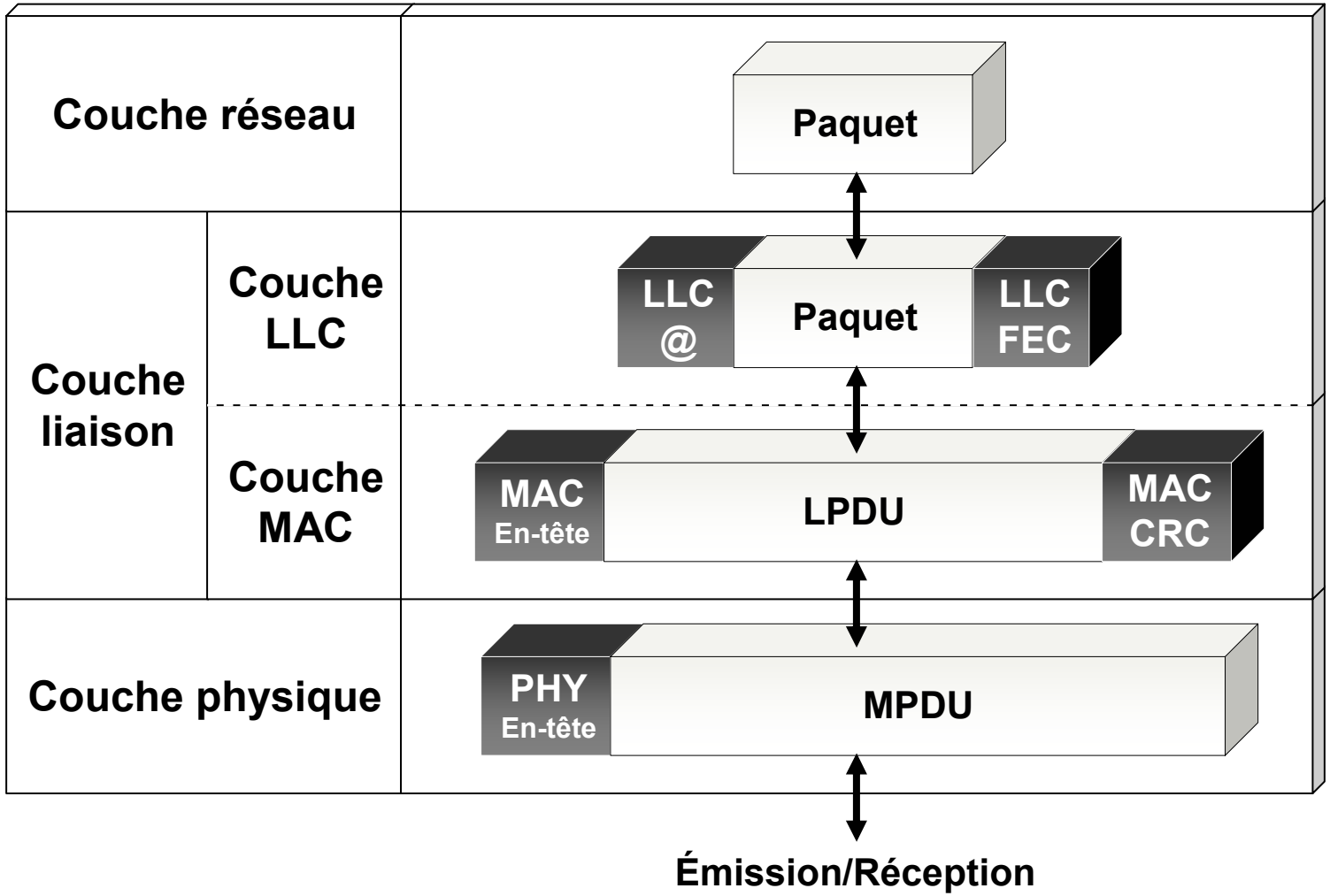
La couche LLC

- 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

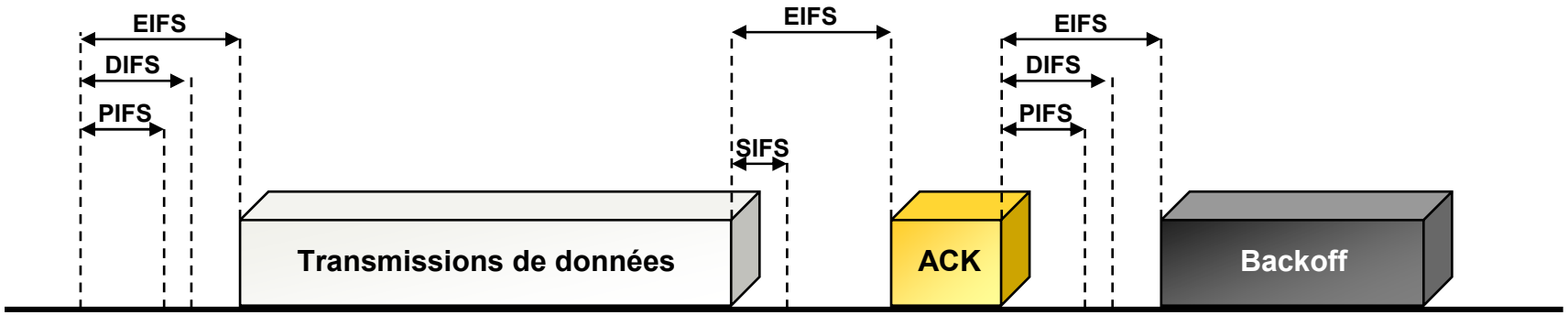
L'écoute du support

- 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
    - 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

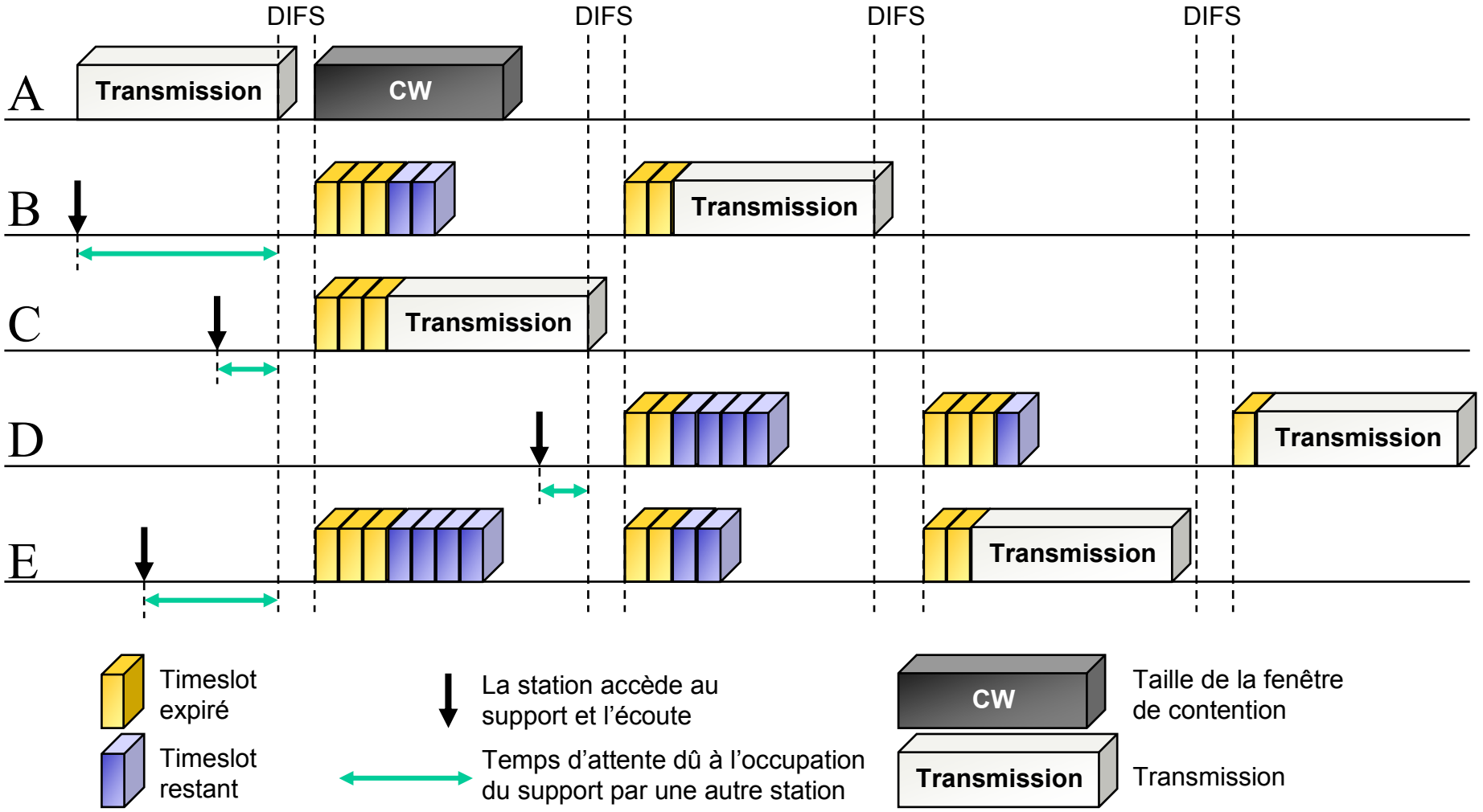
- mécanisme d'espacement entre deux trames : IFS
- 4 types d'*Inter-Frame Spacing* :
  - **SIFS : *Short IFS* :** sépare les différentes trames d'un même dialogue (données et ACK, RTS et CTS, différents fragments d'une trame segmentée, trame de polling en mode PCF)
  - **PIFS : PCF IFS** = SIFS + 1 timeslot : 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

Le *back-off*

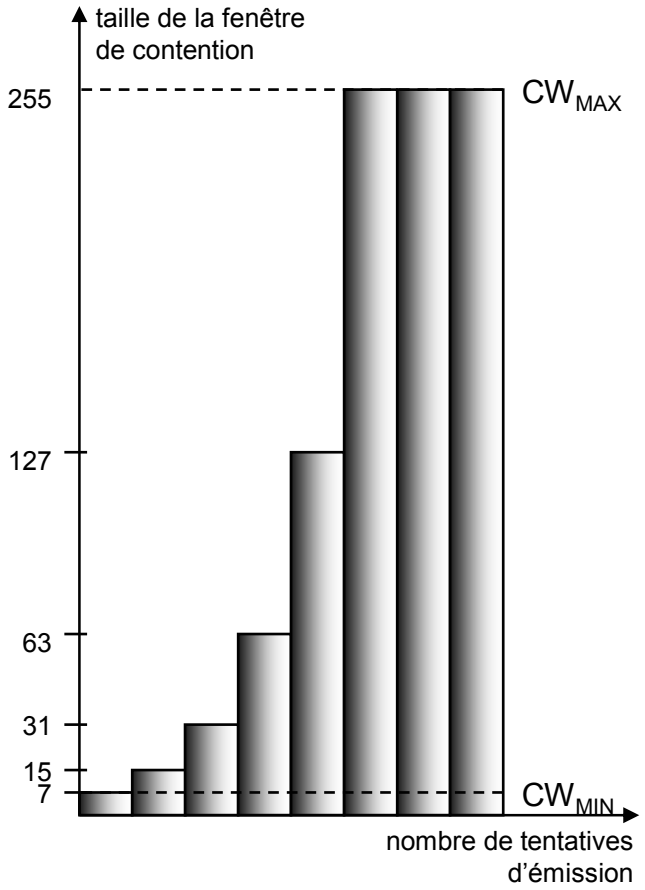
- fenêtre de contention CW, et un *timer* $T_{backoff}$=random(0,CW)×timeslot



Distributed Coordination Function

La contention

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



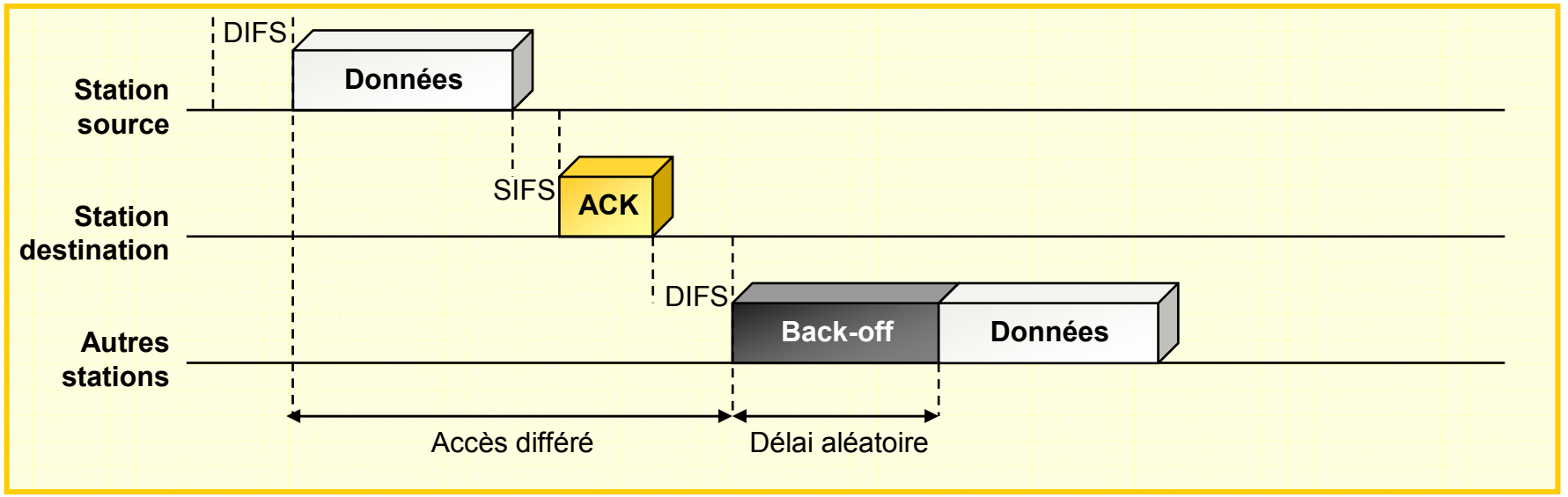
- le tirage au sort de la durée d'attente s'effectue sur un intervalle plus grand
- deux stations qui sont entrées en collision ont une probabilité plus faible mais non nulle d'entrer à nouveau en collision
- $n^{ième}$ tentative de transmission :

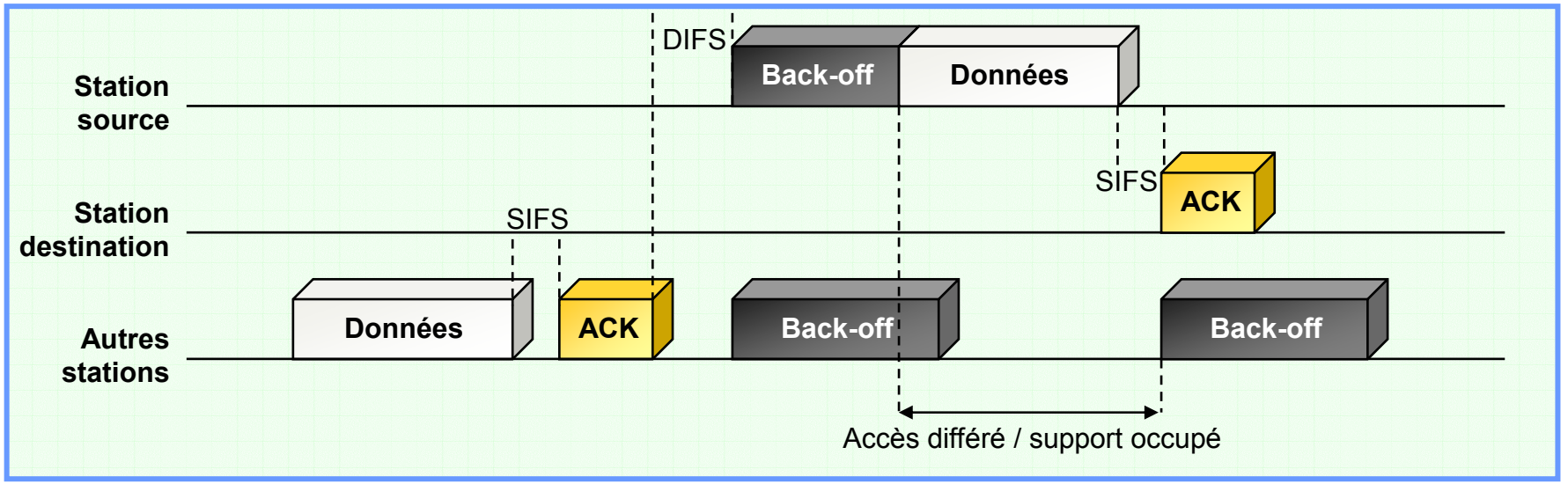
$$T_{backoff}(i) = random(0,CW_i) \times timeslot$$

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

Distributed Coordination Function

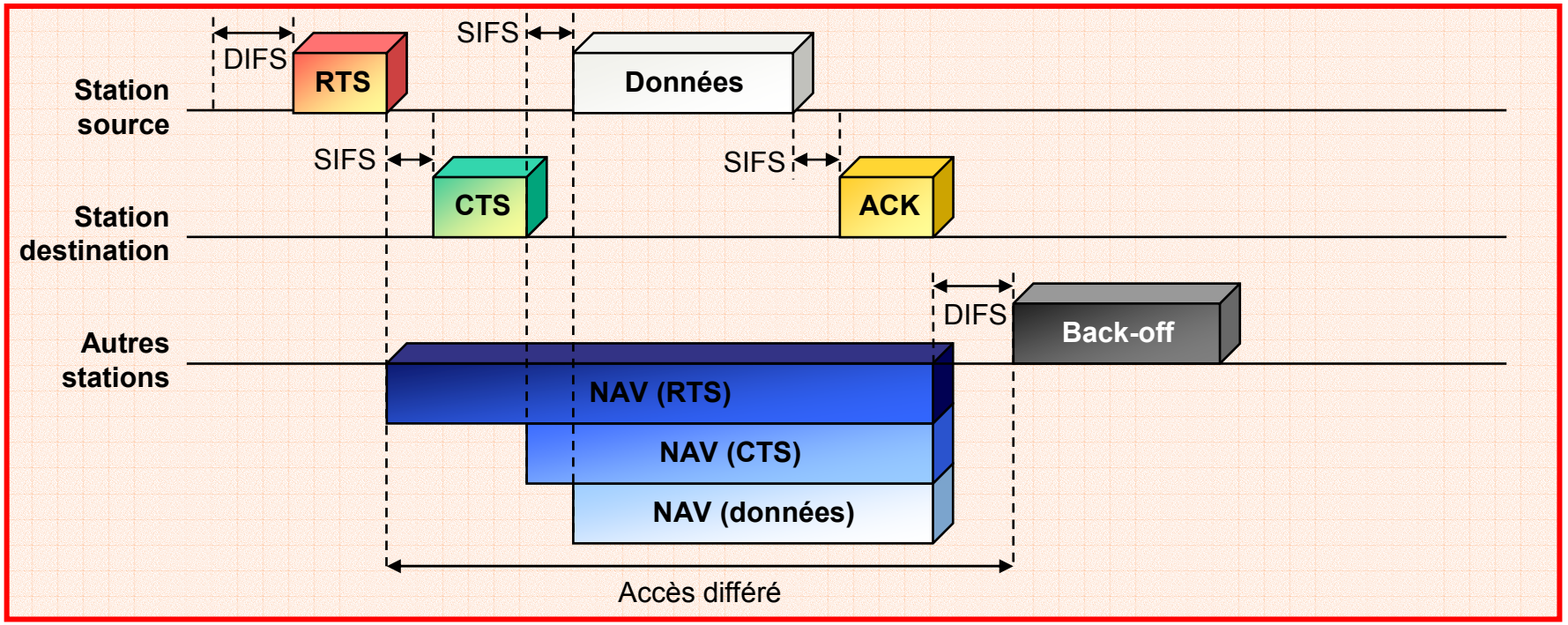
Exemples de transmissions





Distributed Coordination Function

Exemples de transmissions avec réservation



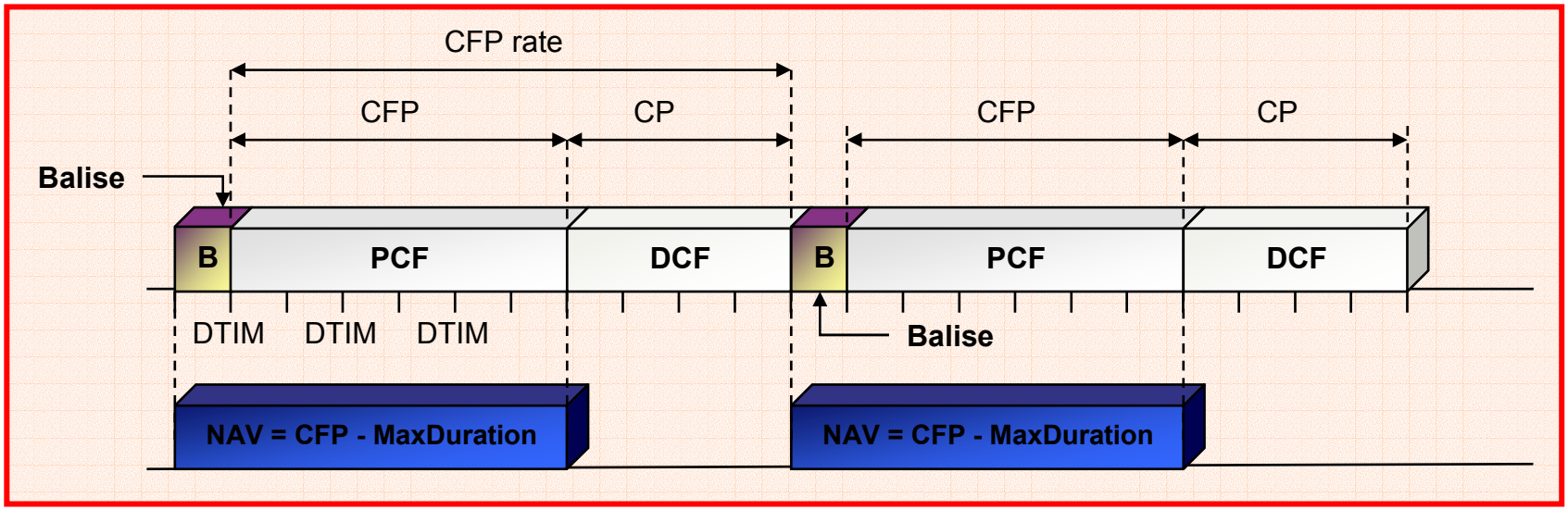
Point Coordination Function

PCF

- 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

Variation du débit

Gestion de la mobilité

Qualité de service

Économie d'énergie

Fragmentation et réassemblage

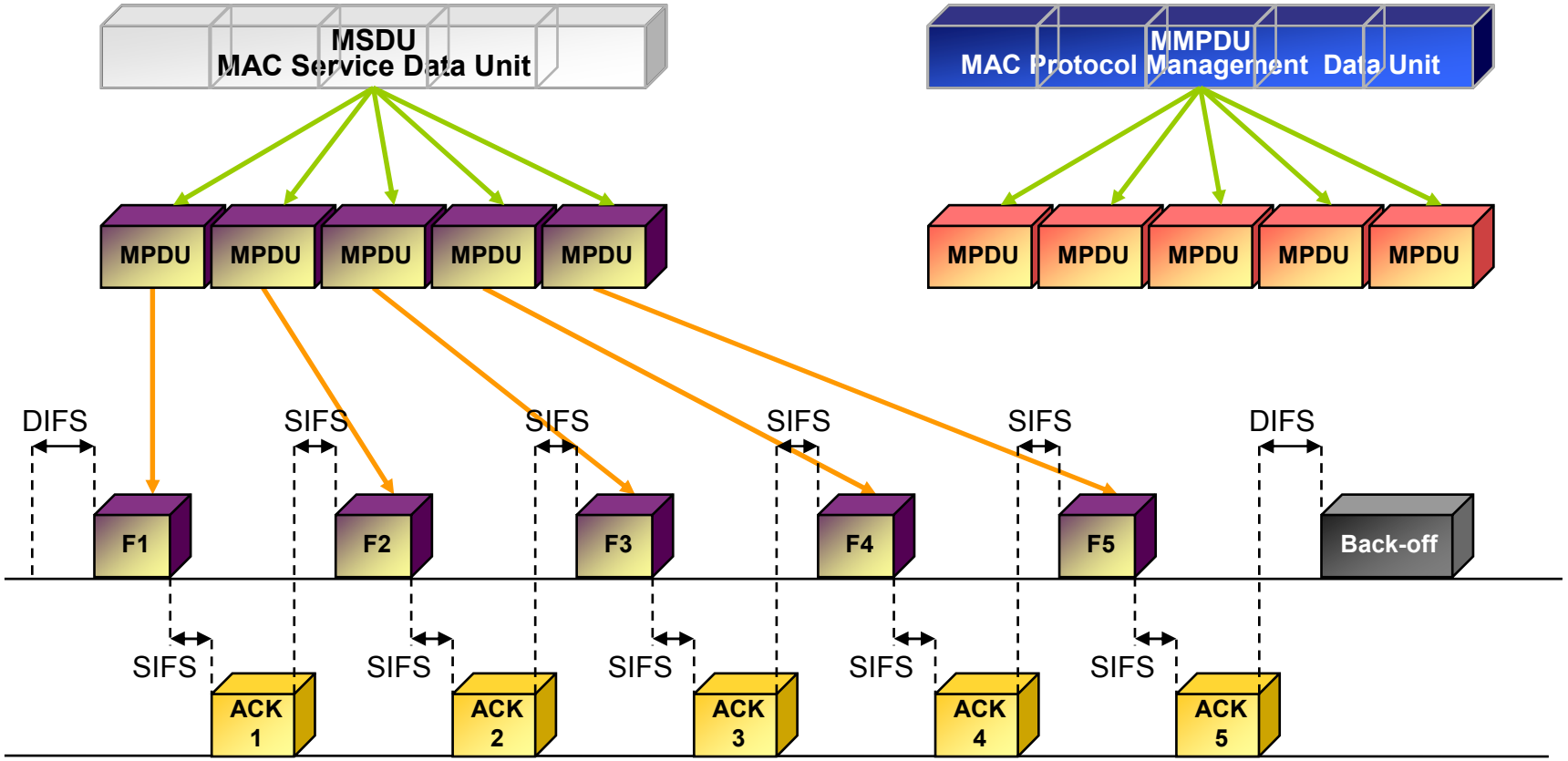
- Taux d'erreur pour liaison sans fil très supérieur à celui des liaisons filaires : nécessité de transmettre de petits paquets
- Fragmentation d'une :
  - trame de donnée MSDU (*MAC Service Data Unit*)
  - trame de gestion MMPDU (*MAC Management Protocol Data Unit*)
  - en plusieurs trames MPDU (*MAC 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

Mécanisme d'émission d'une trame fragmentée

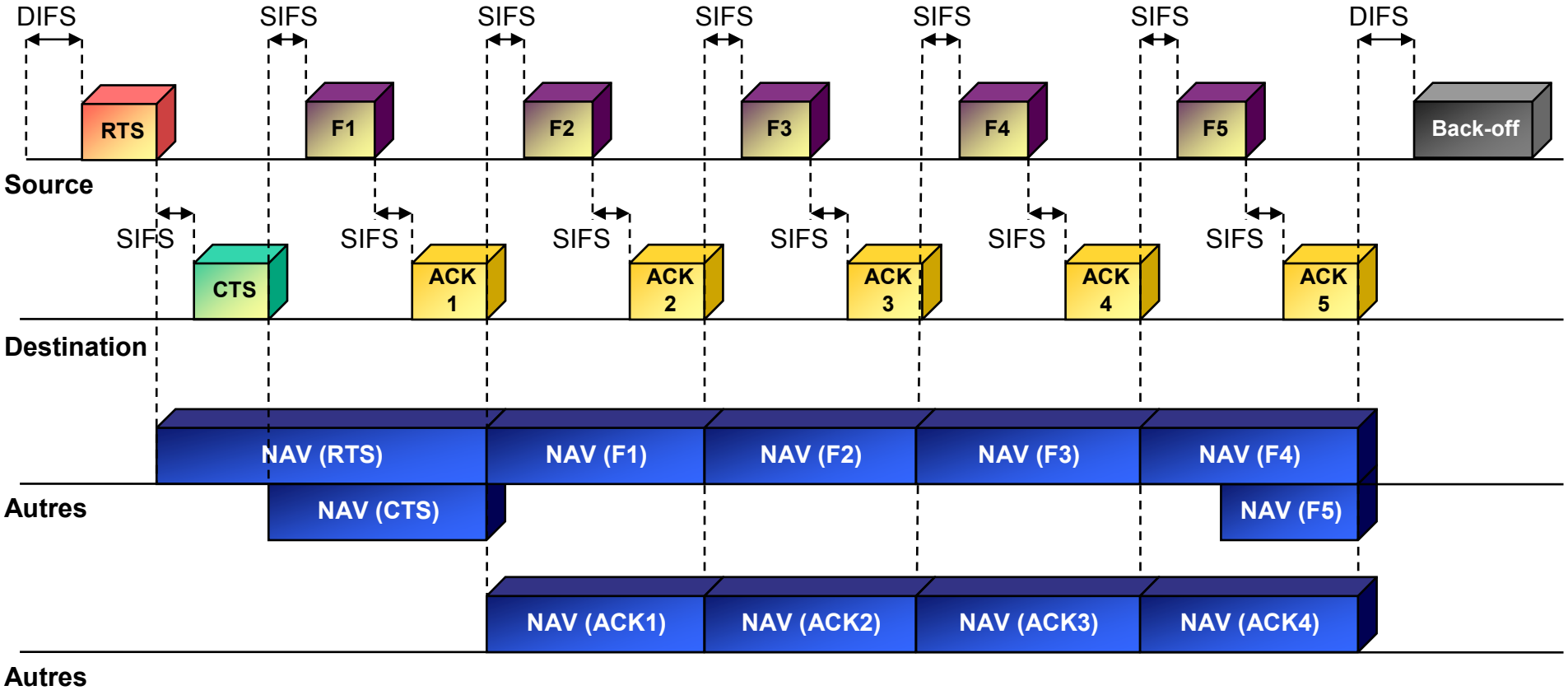
Fragmentation d'une trame de donnée

Fragmentation d'une trame de gestion



Fragmentation et réassemblage

Émission d'une trame fragmentée avec réservation du support

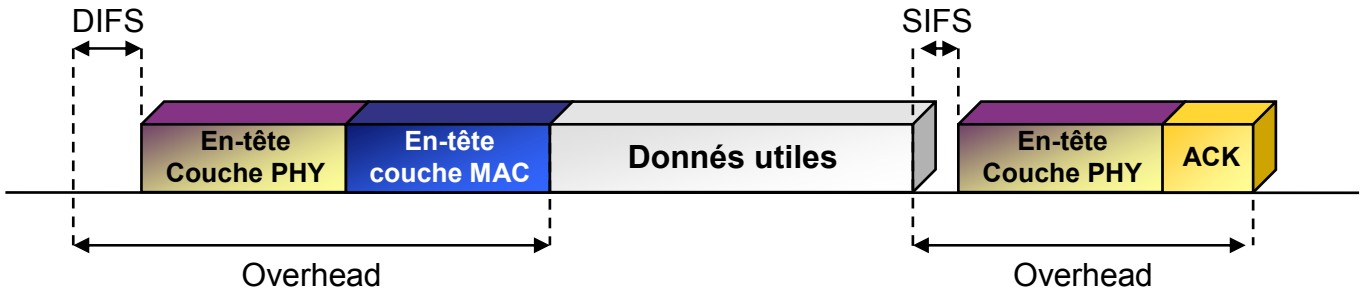


Fragmentation et réassemblage

- 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 11 Mbits/s
- 11 Mbits/s donne un débit utile de 6 Mbits/s soit 0,75 Mo/s
- 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
- 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

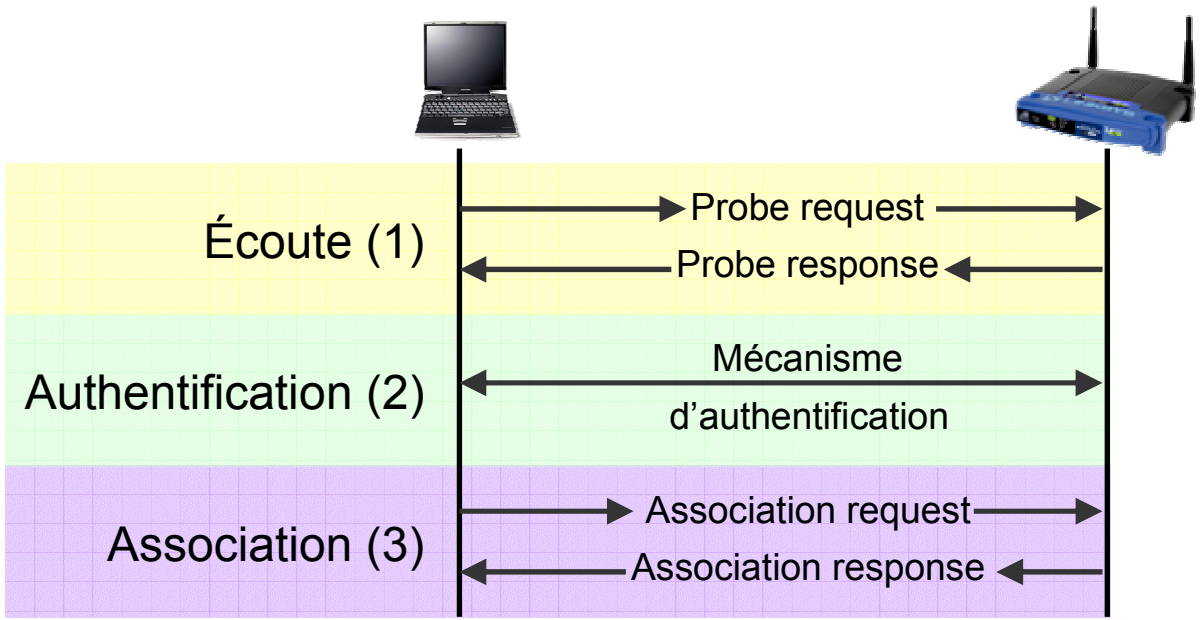
Gestion de la mobilité

- 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

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



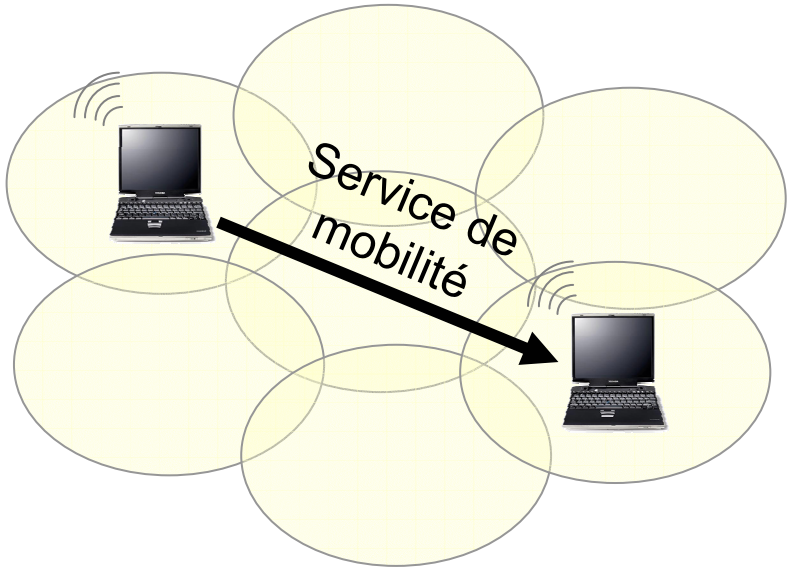
Réassociation

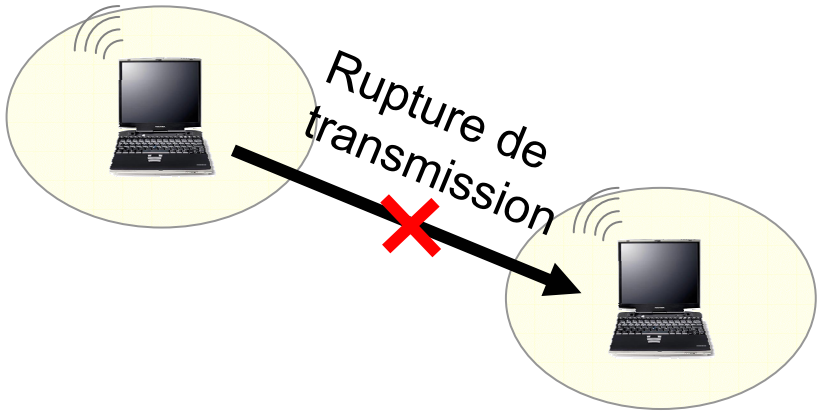
- similaire à l'association, effectuée lors de changements des caractéristiques de l'environnement (déplacement, trafic élevé)

Gestion de la mobilité

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)



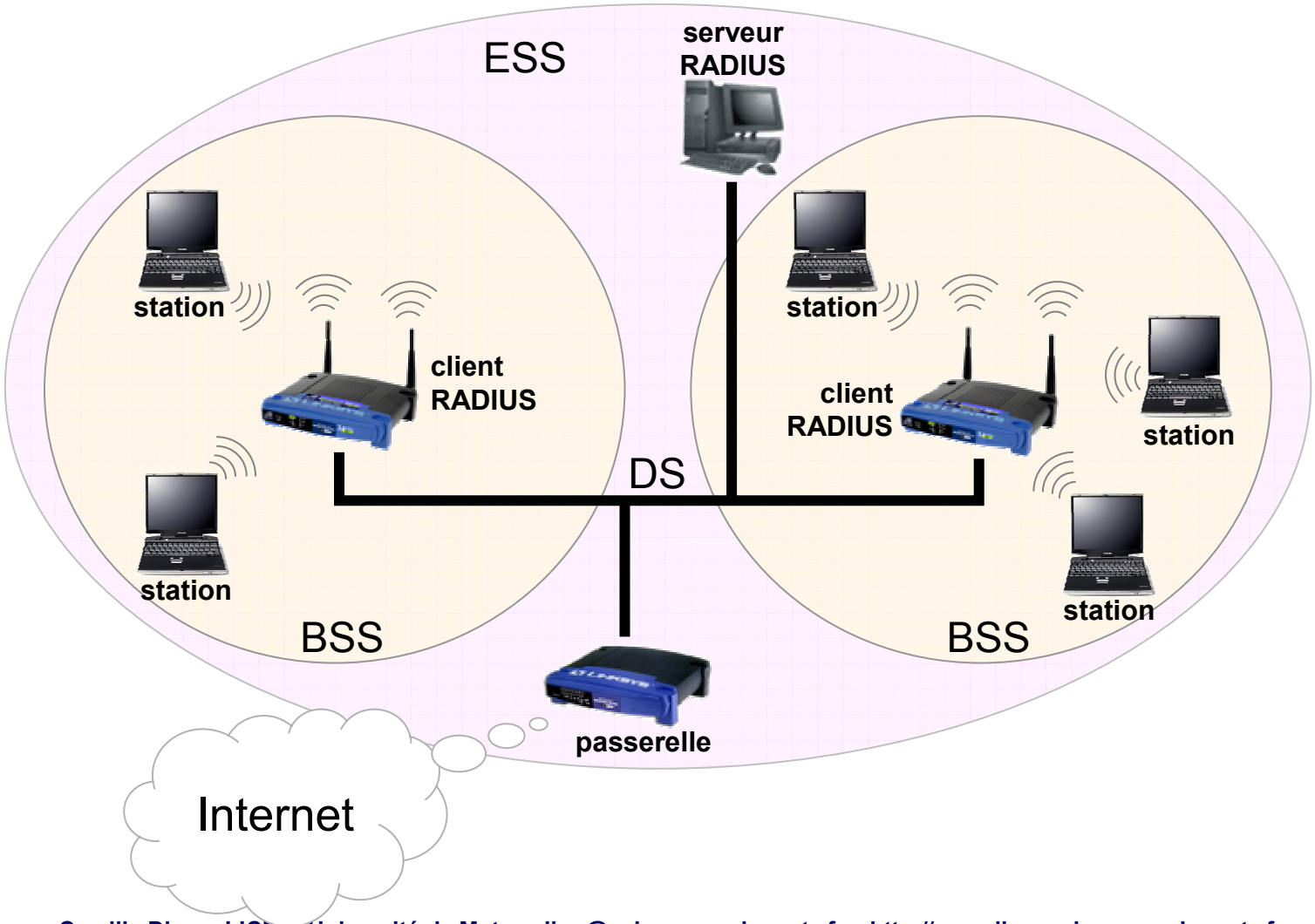


Gestion de la mobilité

- 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

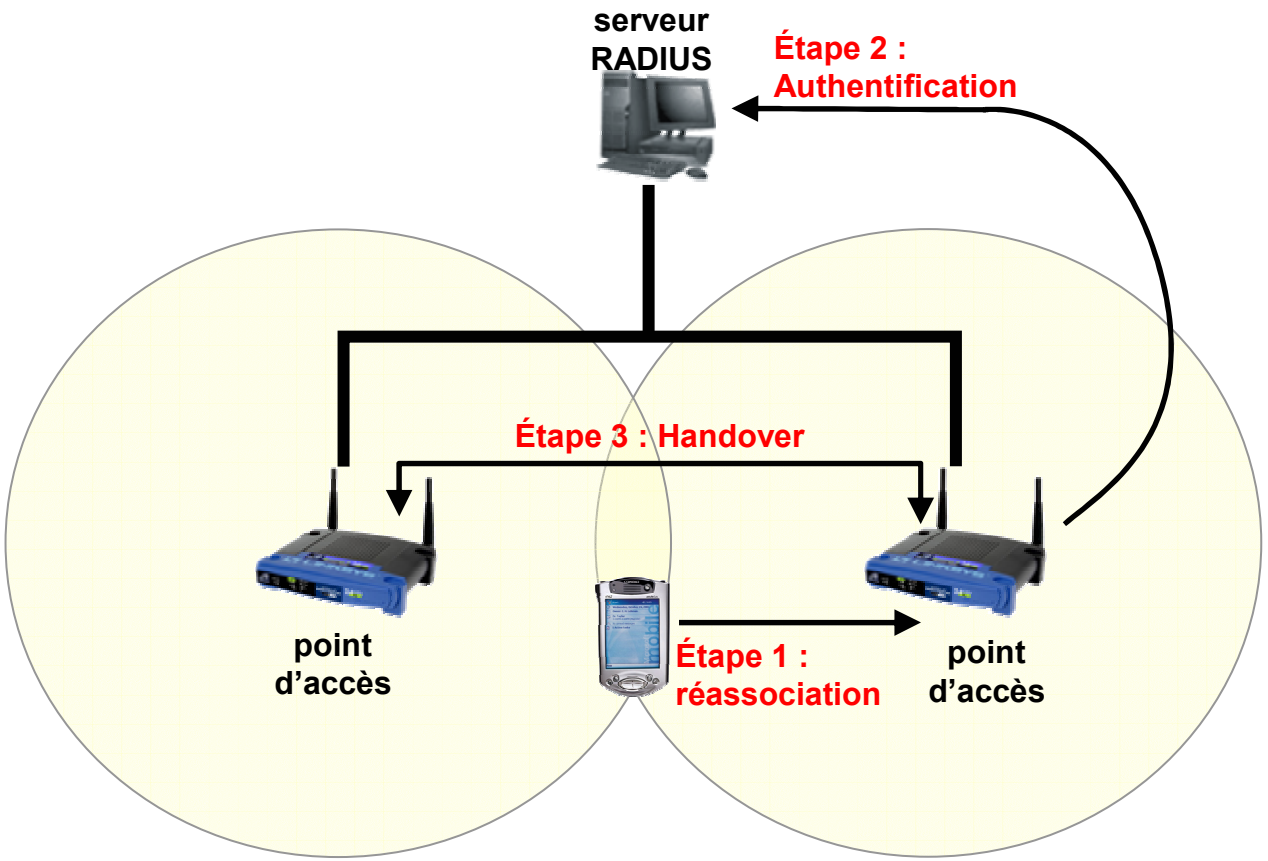
Gestion de la mobilité

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



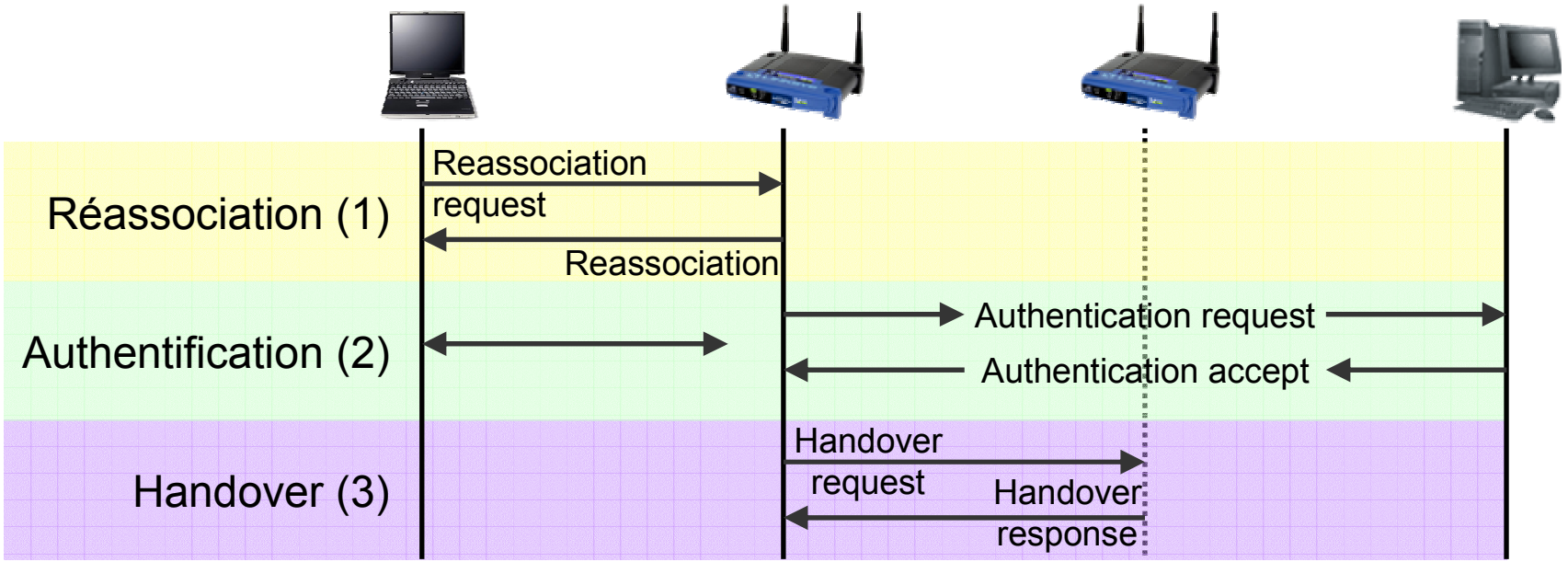
Gestion de la mobilité

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



Gestion de la mobilité

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



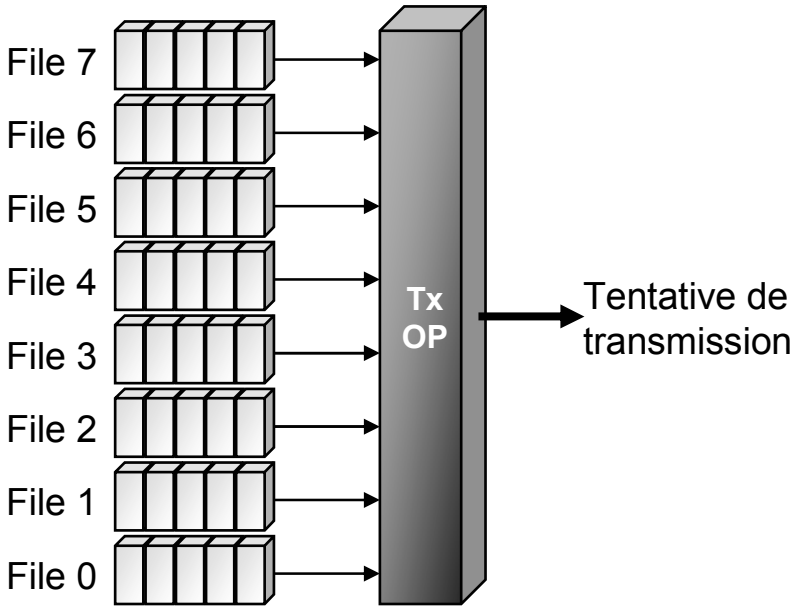
Économie d'énergie

- 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

Qualité de service

Gestion des priorités : accès EDCF (*Extended DCF*)

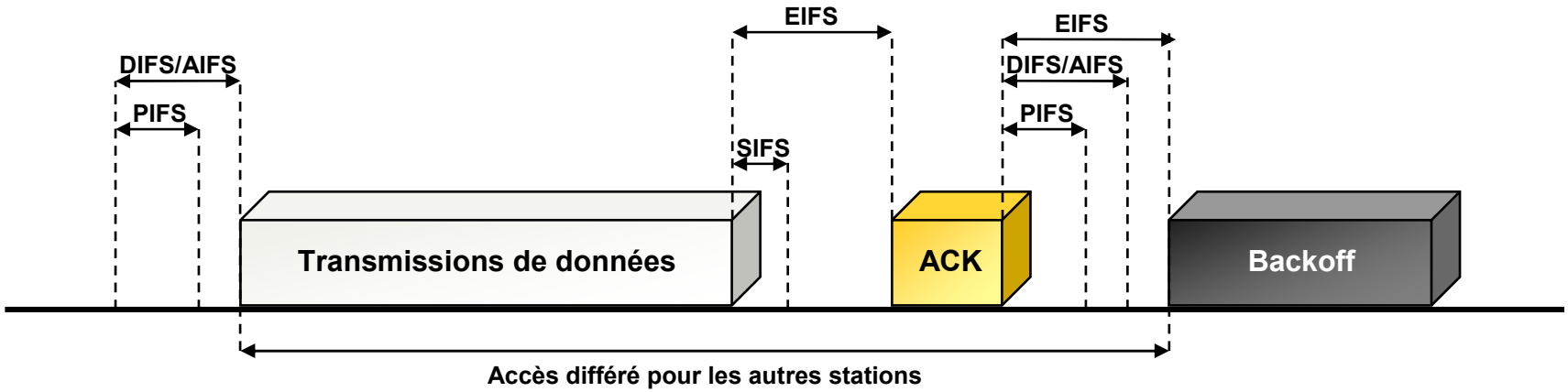
- méthode PCF jamais utilisée car non implantée par les fabricants
- EDCF : évolution du DCF, introduite dans IEEE 802.11e
- accès au support selon le niveau de priorité de la trame
- 8 niveaux de priorité : 8 files d'attente de transmission
- mécanisme TxOP : *Transmission Opportunities*



Qualité de service

AIFS : *Arbitration IFS*

- utilisé de la même manière que le DIFS
- valeur dynamique : varie en fonction du niveau de priorité requis
- valeur supérieure ou égale au DIFS
- diminue les risques de collision



L'algorithme de back-off

- sa valeur est dynamique également
- variation fonction de la taille de la fenêtre de contention : si la taille est petite, la station attend moins longtemps

Qualité de service

Accès HCF (*Hybrid coordination function*)

- méthode hybride entre l'EDCF et le PCF
- introduite dans IEEE 802.11e
- définit un HC (Hybrid Coordinator) qui génère des bursts de CFP au lieu d'un simple CFP dans le PCF
- système plus centralisé que le PCF

LA SÉCURITÉ

Accès au réseau et chiffrement

Chiffrement des données

Déchiffrement des données

Authentification

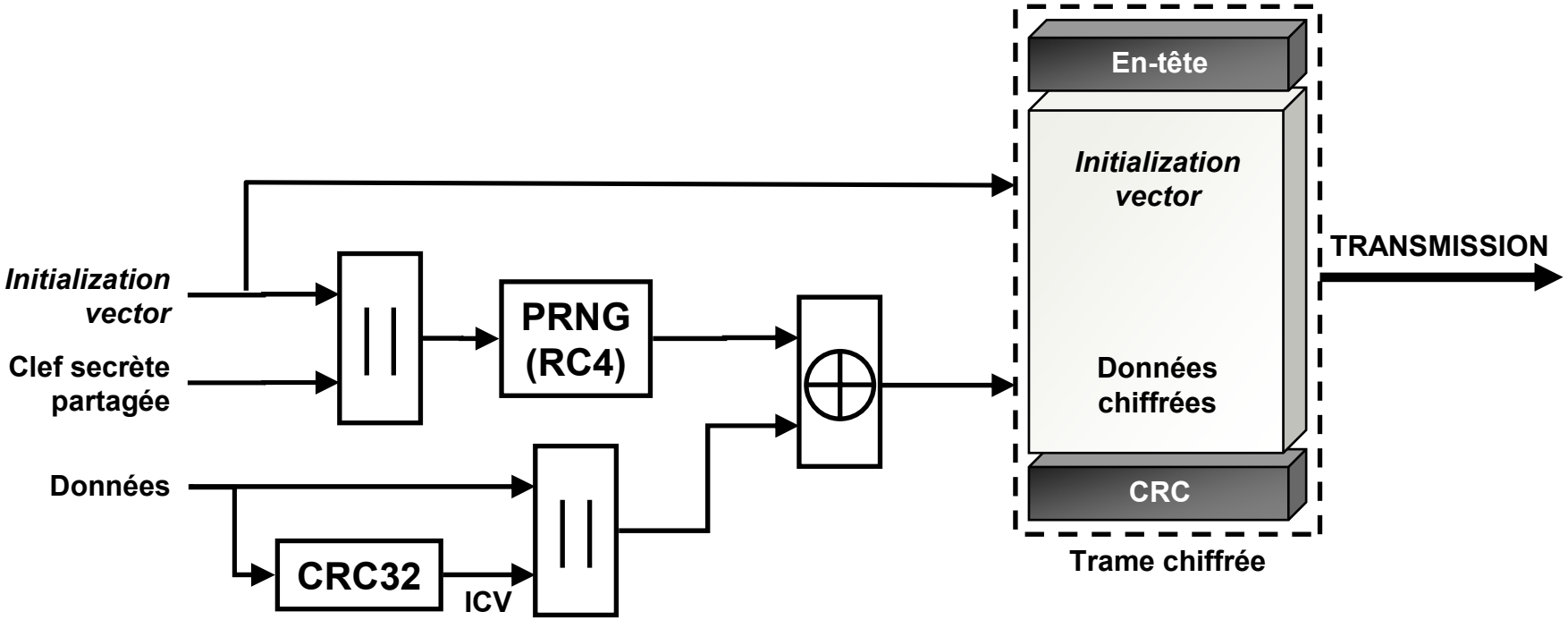
Les failles de sécurité

Accès au réseau et chiffrement

- SSID : seul mécanisme de sécurité obligatoire
- 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
- WEP : *Wired Equivalent Privacy*
  - repose sur RC4 :
    - key scheduling algorithm : clé composée d'une clef secrète partagée concaténée à un *Initialization Vector* (IV) : permet de générer une table d'état
    - séquence pseudo-aléatoire : la table précédente est placée dans un générateur pseudo-aléatoire

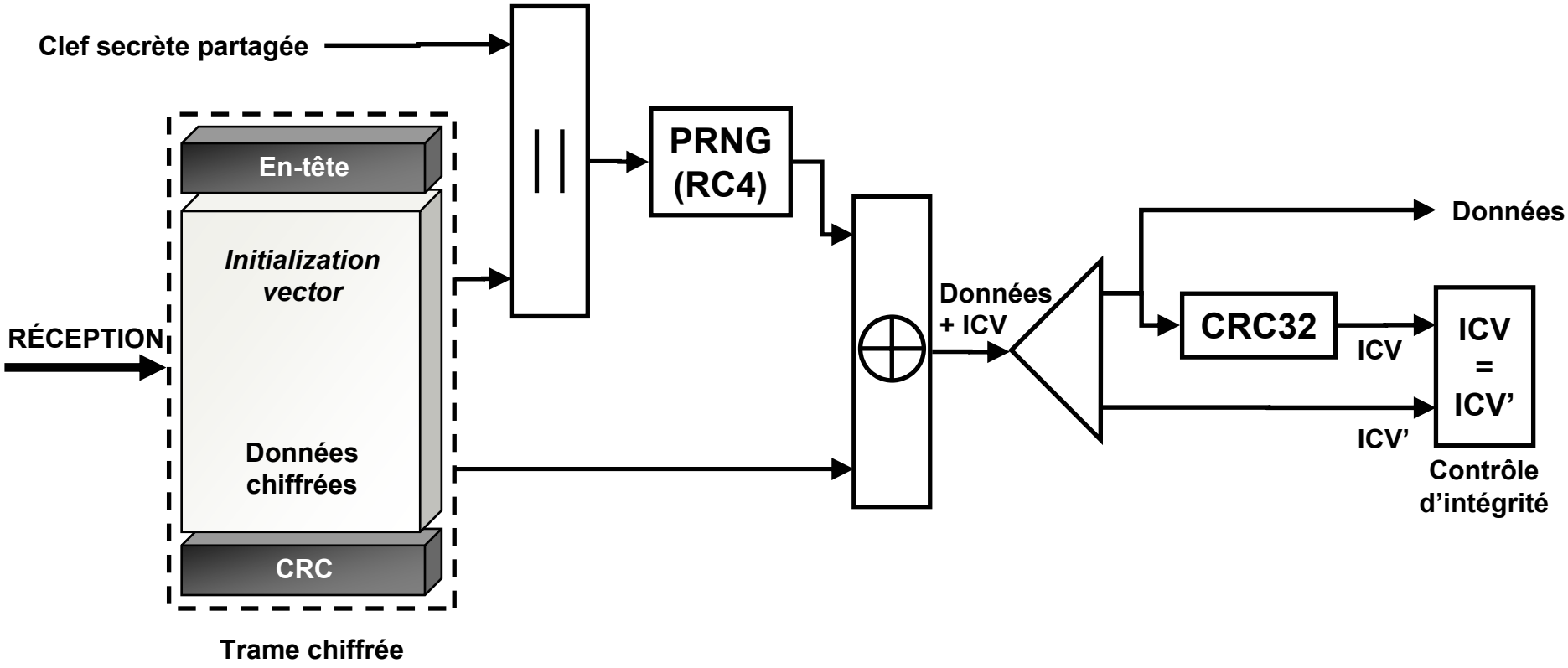
Chiffrement des données

Processus de chiffrement



Déchiffrement des données

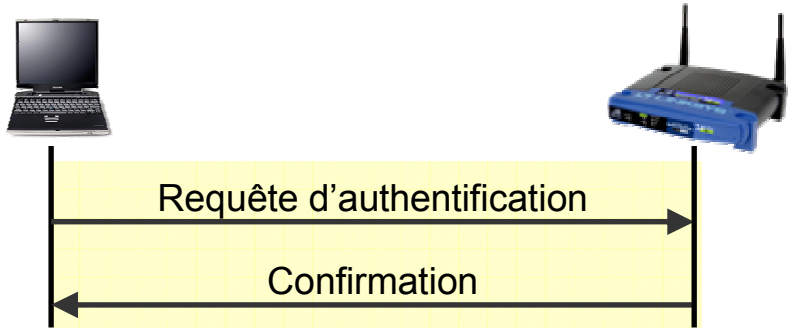
Processus de déchiffrement



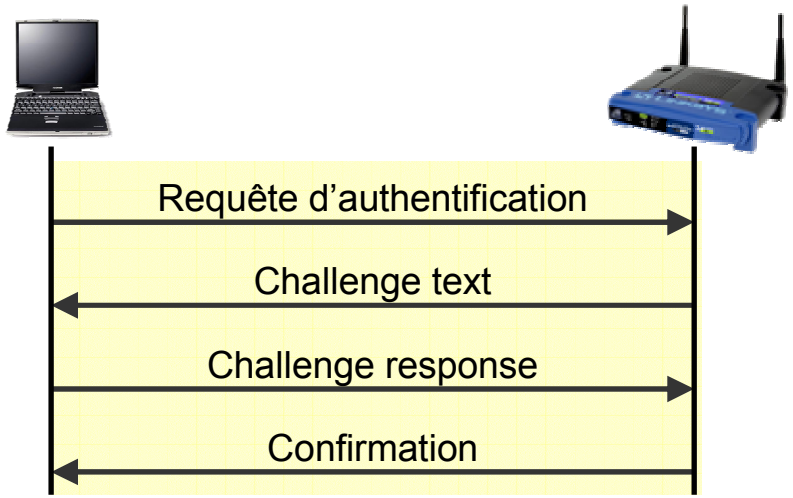
Authentification

2 mécanismes :

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



- ***Shared Key Authentication*** :



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
    - 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

Les failles de sécurité

Réponses futures

- RC4 Fast Packet Keying (WEP+) : clef de chiffrement unique pour chaque trame
- IEEE 802.11i : introduction de l'AES ; plus gourmand en ressources

Solutions actuelles : serveurs d'authentification + tunnels

- IEEE 802.1x : contrôleur + serveur d'authentification
- réseaux privés virtuels (VPN)
- RADIUS
- gestion dynamique des clefs : modifier la clef périodiquement

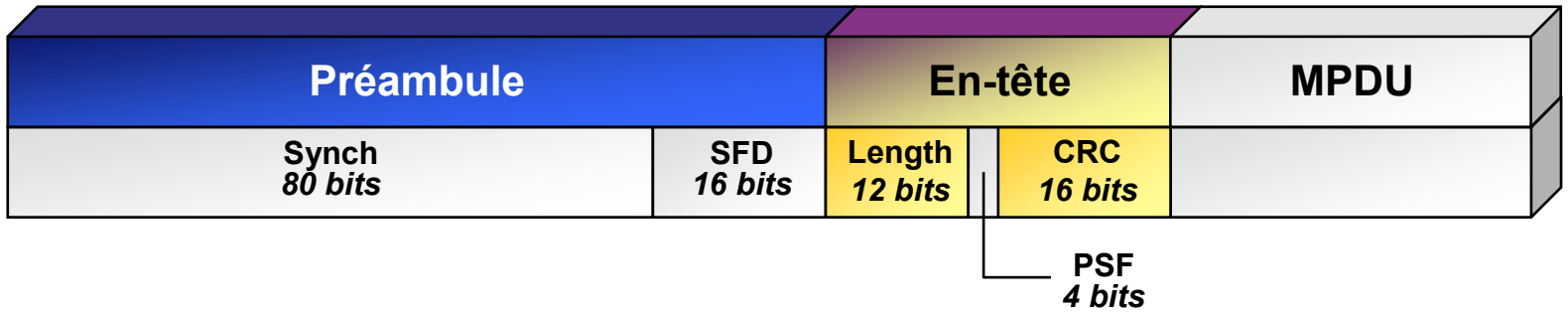
LES TRAMES

Les trames de niveau physique

- PLCP-PDU : *Physical Level Common Protoco – Protocol Data Unit*
- Constituées de trois parties :
  - **préambule** : détection du signal, synchronisation, détection du début de trame, prise du canal radio
  - **en-tête** : diverses informations comme le débit
  - **données** : informations provenant de la couche MAC : MPDU (*MAC Protoco Data Unit*)
- Ces informations varient en fonction de l'interface physique utilisée : FHSS, DSSS, IR, OFDM

Les trames PHY

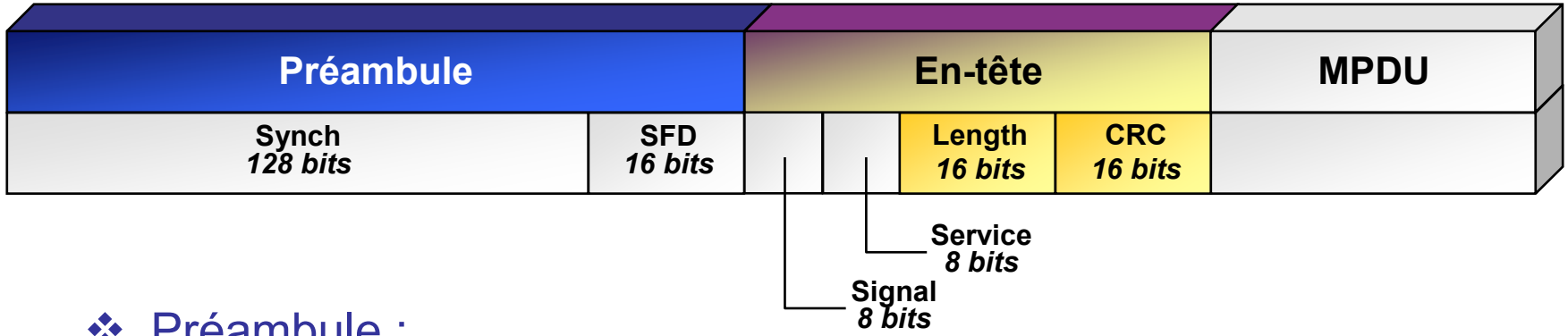
La trame FHSS



- Préambule :
  - **Synch** : séquence de 80 bits alternés (0 et 1) permettant la synchronisation
  - **SFD** (*Start Frame Delimiter)* : suite de 16 bits définissant le début de trame : 0000110010111101
- En-tête :
  - **Length** : nombre d'octets dans la trame, détermine la fin de trame
  - **PSF** (*Payload Signalling Field*) : débit utilisé sur l'interface radio
  - **CRC** (*Cyclic Redundancy Code*) : détection d'erreur

Les trames PHY

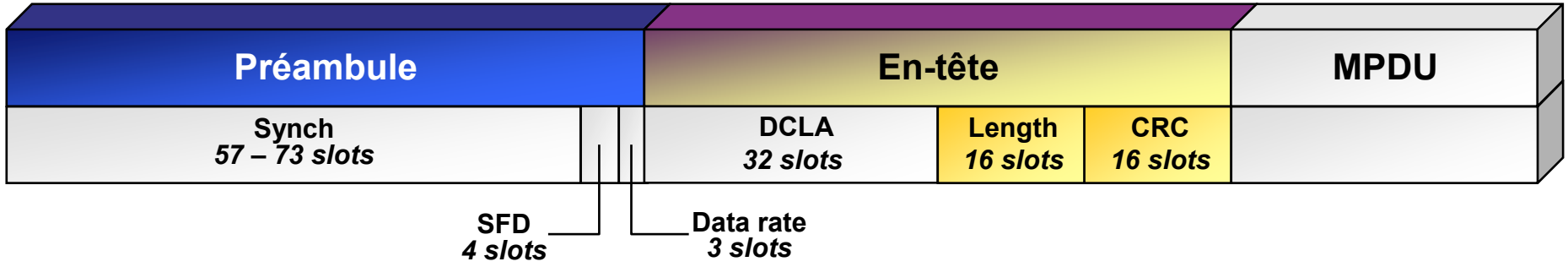
La trame DSSS



- Préambule :
  - **Synch** : détection et synchronisation
  - **SFD** (*Start Frame Delimiter)* : début de trame
- En-tête :
  - **Signal** : débit utilisé sur l'interface radio
  - **Service** : réservé pour un usage futur : ne contient que des 0
  - **Length** : nombre d'octets dans la trame , détermine la fin de trame
  - **CRC** (*Cyclic Redundancy Code*) : détection d'erreur

Les trames PHY

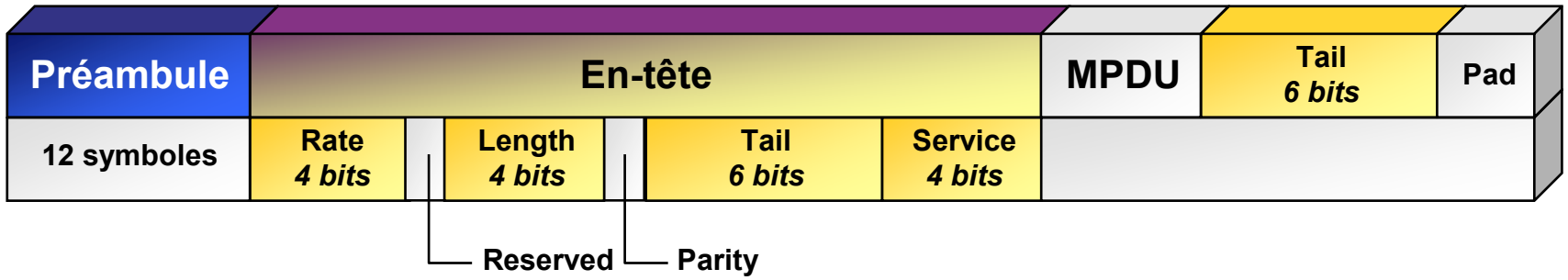
La trame IR



- Préambule :
  - **Synch** : détection et synchronisation
  - **SFD** (*Start Frame Delimiter)* : début de trame
- En-tête :
  - **Data rate** : débit utilisé sur l'interface infrarouge
  - **DCLA** (*Data Control Level Adjustement*) : permet d'ajuster la vitesse
  - **Length** : nombre d'octets dans la trame, détermine la fin de trame
  - **CRC** (*Cyclic Redundancy Code*) : détection d'erreur

Les trames PHY

La trame OFDM

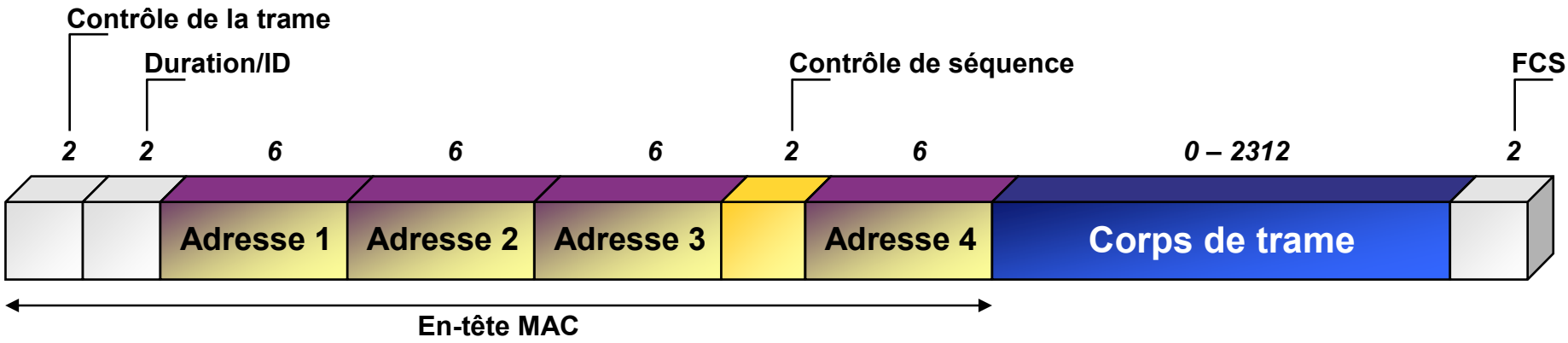


- Préambule différent : 12 symboles
- En-tête :
  - **Rate** : débit utilisé sur l'interface OFDM
  - **Reserved** : réservé pour un usage future ; ne contient que des 0
  - **Length** : nombre d'octets dans la trame, détermine la fin de trame
  - **Parity** : calcul de parité, détection d'erreur
  - **Tail** : « queue », réservé pour un usage future ; ne contient que des 0
  - **Service** : réservé pour un usage future ; ne contient que des 0

Les trames MAC

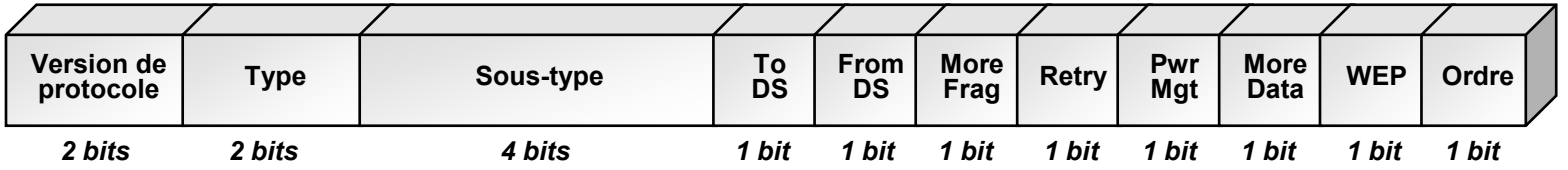
Trois types de trames MAC :

- **trames de données** : transmission des données
- **trames de contrôle** : contrôle de l'accès au support (RTS, CTS, ACK, etc.)
- **trames de gestion** : association, réassociation, synchronisation, authentification



Les trames MAC

Le champ « contrôle de trame »



- **Version de protocole** : actuellement fixé à 0
- **Type** et **sous-type** : 3 types de trames, plusieurs sous-types
- **To DS** et **From DS** : trame envoyée vers le ou provient du destinataire
- **More fragments**
  - =1 si trame fragmentée et ce n'est pas le dernier fragment
  - =0 si trame non fragmentée ou dernier fragment
- **Retry** =1 si retransmission
- **Power management** : mode économie d'énergie (=1) ou actif (=0)
- **More data** : trames présentes en mémoire tampon
- **WEP** : trame chiffrée ou non (trame donnée ou gestion/authentification)
- **Order** : classe de service strictement ordonnée (*Strictly Ordered Service Class*)

Les trames MAC

Le champ « duration/ID »

- deux sens différents :
  - certaines trames de contrôle : identifiant de la station (AID : *Association IDentity*)
  - toutes les autres trames : valeur de durée de vie utilisée pour le calcul du NAV ; varie de 0 à 32767

Les champs « adresse »

- toutes de longueur 6 octets
- même format que les adresse IEEE 802 MAC
- composées de quatre parties :
  - ***Individual/Group*** (I/G) : premier bit : adresse individuelle ou de groupe
  - ***Universal/Local*** (U/L) : deuxième bit : adresse locale ou universelle
  - ***Organizationally Unique Identifier*** : 22 bits : assignés par l'IEEE
  - **Numéro de série** : 24 bits : généralement défini par le constructeur

Les trames MAC

Les champs « adresse »

- 2 types d'adresses de groupe :
  - **adresse broadcast** : l'ensemble des stations d'un réseau, 48 bits à 1
  - **adresse multicast** : groupe de stations en nombre fini
- 5 types d'adresses :
  - BSSID (Basic Service Set Identifier) :
    - dans un BSS : adresse MAC
    - dans un IBSS : BSSID de l'IBSS
    - trames de gestion Probe Request : tous les bits à 1
  - DA (Destination Address) : destination de la trame ; indiv. ou de groupe
  - SA (Source Address) : source de la trame ; toujours individuelle
  - RA (Receiver Address) : destination des données ; indiv. ou de groupe
  - TA (Transmitter Address) : source des données ; toujours individuelle

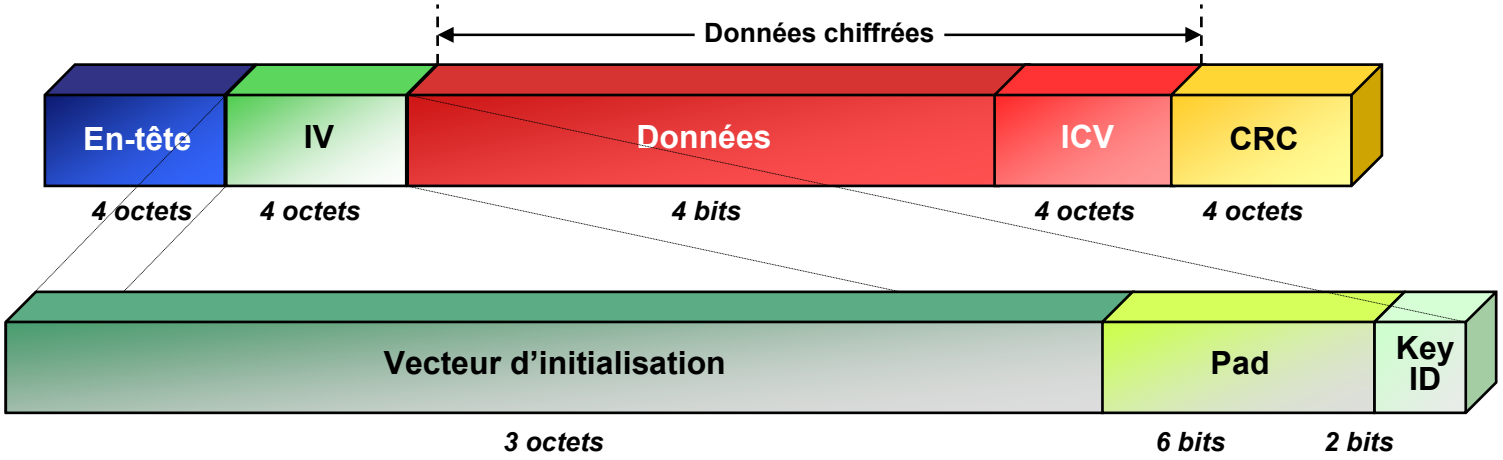
To DS	From DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	Aucun
0	1	DA	BSSID	SA	Aucun
1	0	BSSID	SA	DA	Aucun
1	1	RA	TA	DA	SA

Les trames MAC

- Le champ « contrôle de séquence »
  - **numéro de séquence** (12 bits) : attribué à chaque trame ; initialisé à 0 puis incrémenté pour chaque nouvelle trame
  - **numéro de fragment** (4 bits) : initialisé à 0 puis incrémenté pour chaque nouveau fragment
- Les données et le corps de la trame
  - taille minimale nulle (trames de gestion ou de contrôle)
  - taille maximale 1500 octets
  - taille plus importante si chiffrée par WEP
  - *Initialization Vector* (IV)
  - *Integrity Check Value* (ICV)
- Le champ FCS *(Frame Check Sequence)*
  - CRC sur 32 bits pour contrôler l'intégrité des trames

Les trames MAC chiffrées

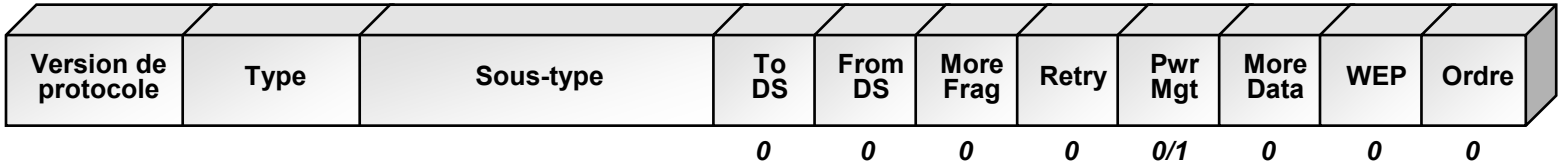
Une trame n'est chiffrée que partiellement :



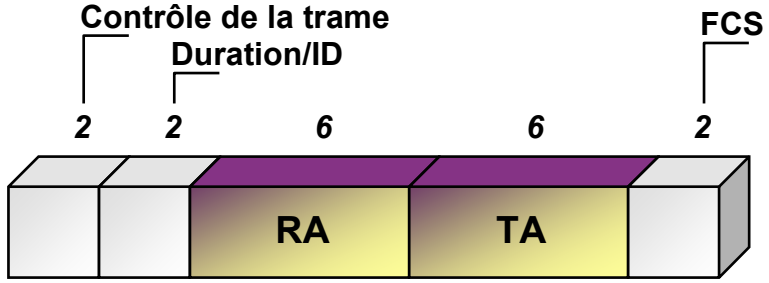
- **IV** : vecteur d'initialisation défini dans le WEP
- **Pad** : ne contient que des 0
- **Key ID** : valeur d'une des 4 clefs permettant de déchiffrer la trame

Les trames de contrôle

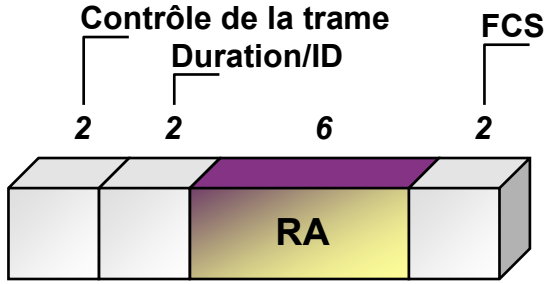
Trame de contrôle :



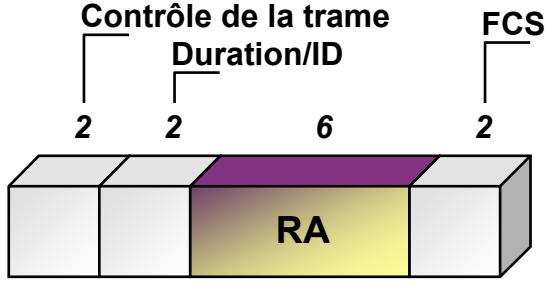
Trame RTS :



Trame CTS :

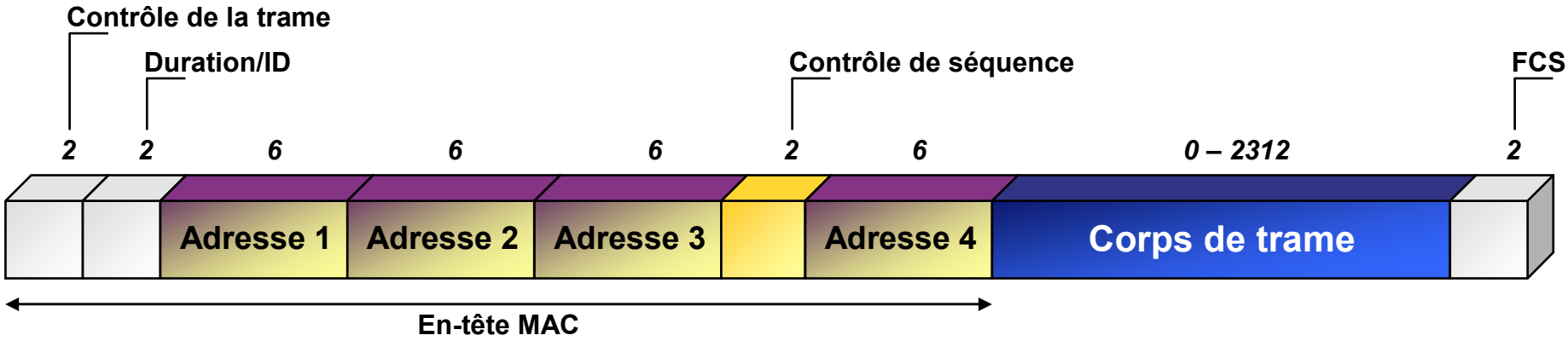


Trame ACK :

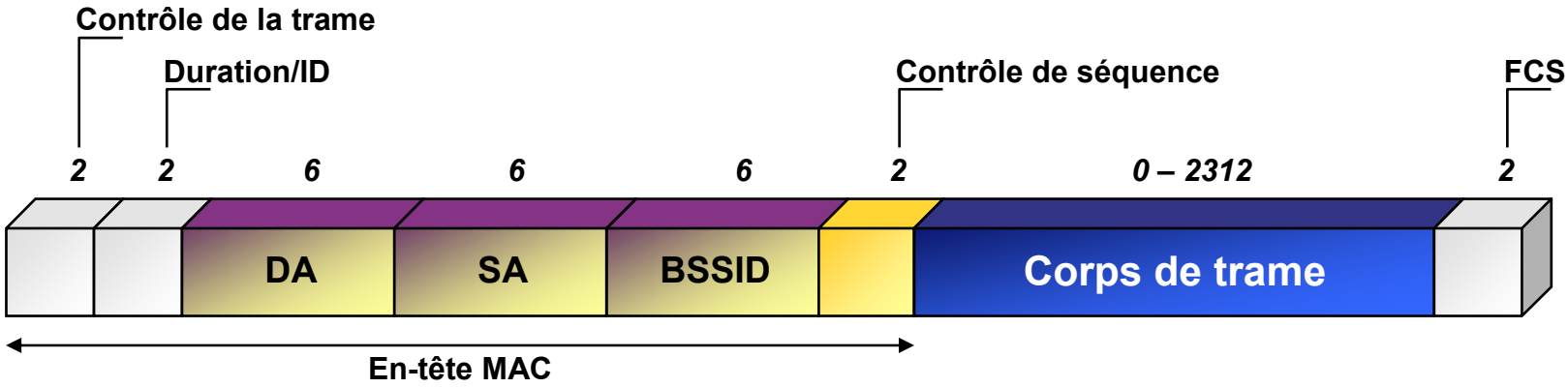


Les trames de gestion et donnée

Trame de gestion :



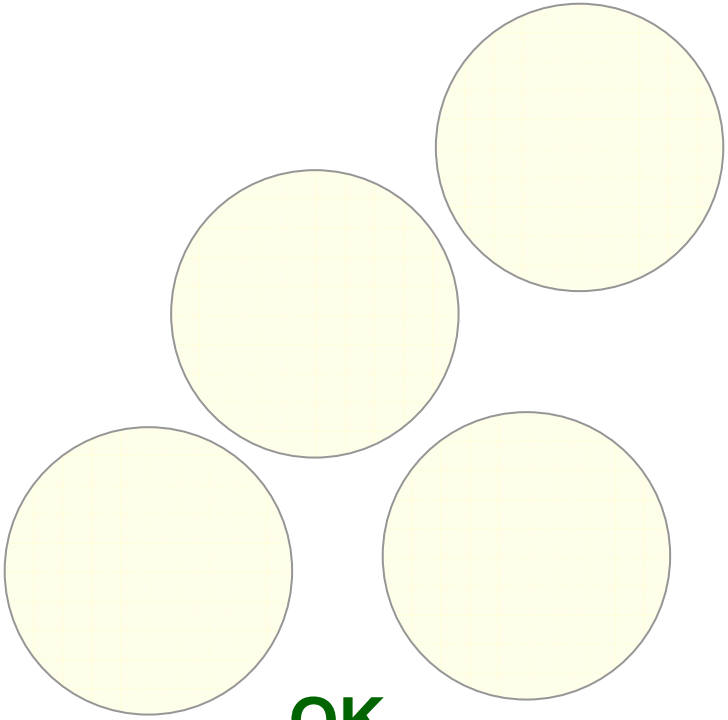
Trame de donnée :



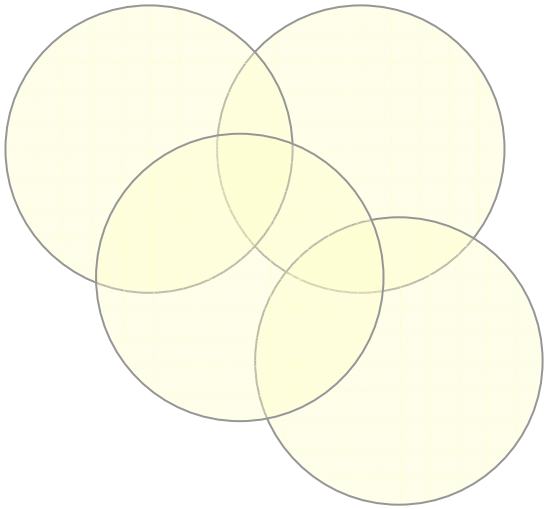
CONFIGURATION ET INSTALLATION

Affectation des canaux

- 14 canaux dans la bande ISM : 2,4 – 2,4835 GHz
- 4 canaux dans la bande 2,446 – 2,4835 GHz
- Affectation d'un canal unique ou de plusieurs canaux non recouvrant ne pose pas de problèmes



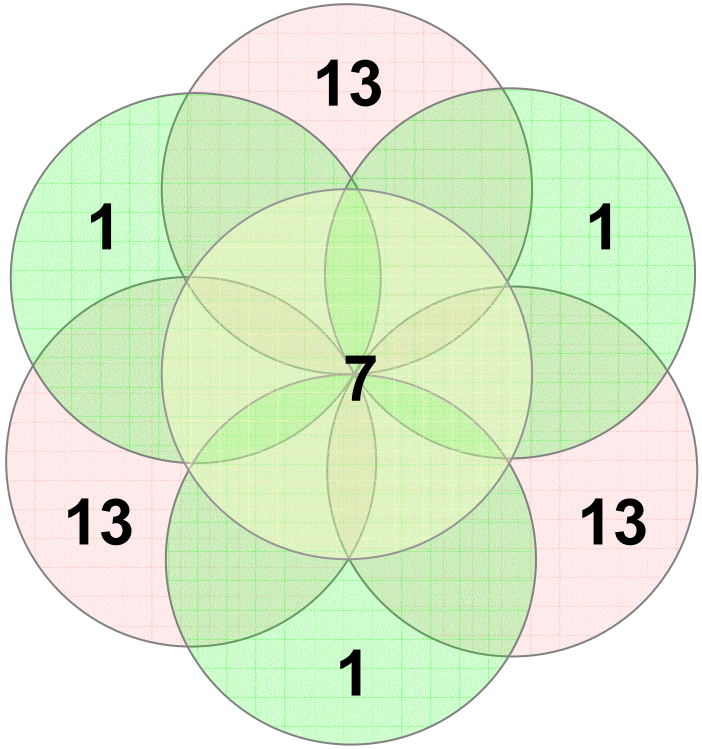
OK



Problème

Affectation des canaux

- Exemple d'affection à 7 points d'accès de 3 canaux qui ne se perturbent pas mutuellement :

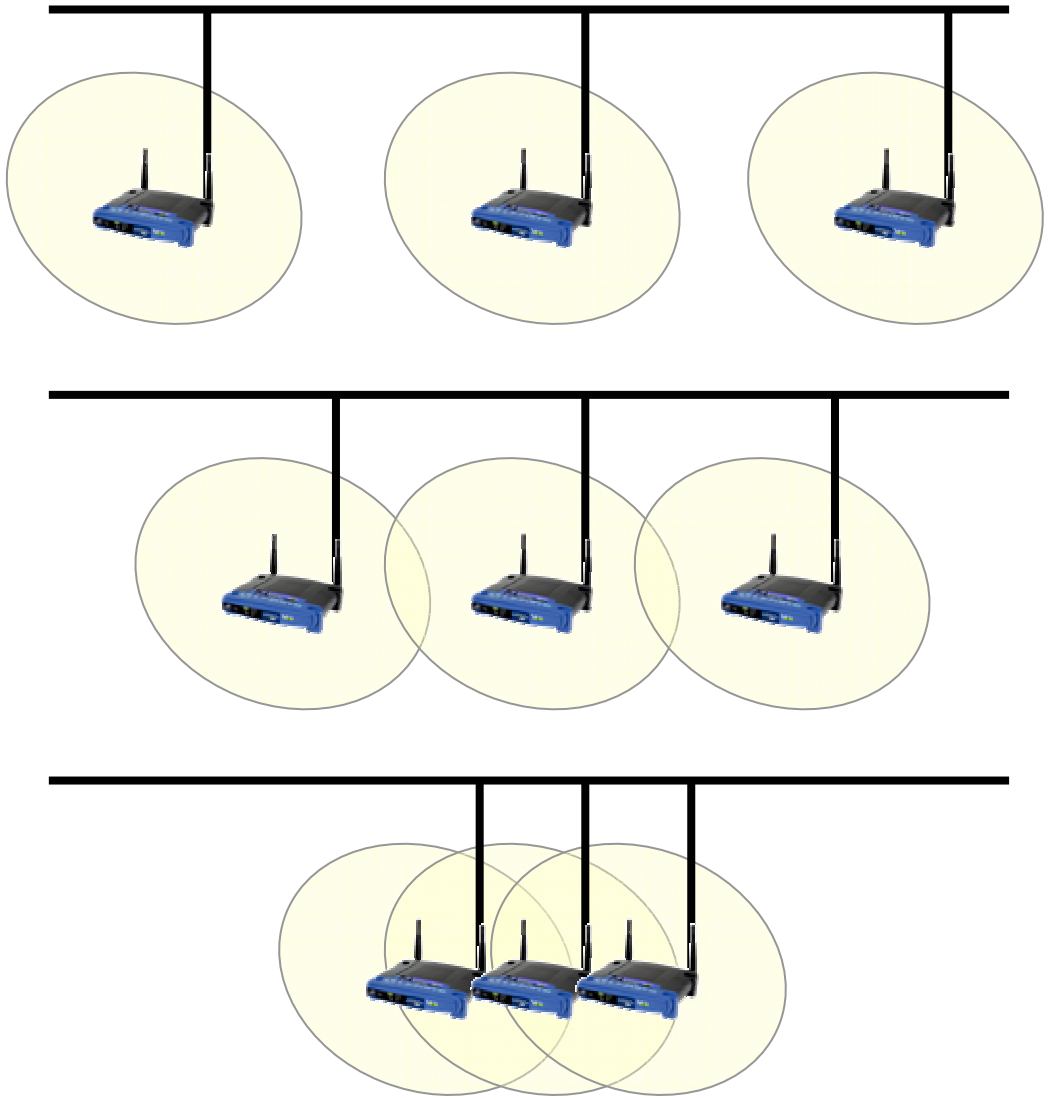


- Autre possibilité : 1, 6 et 11
- Même si on dispose de 14 canaux, seuls 3 peuvent être utilisés si on a plusieurs points d'accès

Affectation des canaux

- Puissance autorisée :
  - Totalité bande ISM : 10 mW ; taille cellule = 15 m
  - Canaux 10-13 : 100 mW ; taille cellule = 100 m
- Impossibilité de créer des réseaux WiFi important utilisant la topologie en « rosace »

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

Bibliographie

- Davor Males & Guy Pujolle, ***WiFi par la pratique***, Eyrolles, 2002
- IEEE Computer Society, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements*
  - ANSI/IEEE Std 802.11, ***Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications***, 1999
  - ANSI/IEEE Std 802.11a, ***Amendment 1: High-speed Physical Layer in the 5 GHz Band*** , 1999
  - ANSI/IEEE Std 802.11b, ***Amendment 2: Higher-Speed Physical Layer Extension in the 2.4 GHz Band***, 1999
  - ANSI/IEEE Std 802.11b, ***Amendment 2: Higher-speed Physical Layer (PHY) extension in the 2.4 GHz band — Corrigendum 1***, 2001
  - ANSI/IEEE Std 802.11d, ***Amendment 3: Specification for operation in additional regulatory domains***, *2001*