IEEE 802.11 (WiFi)

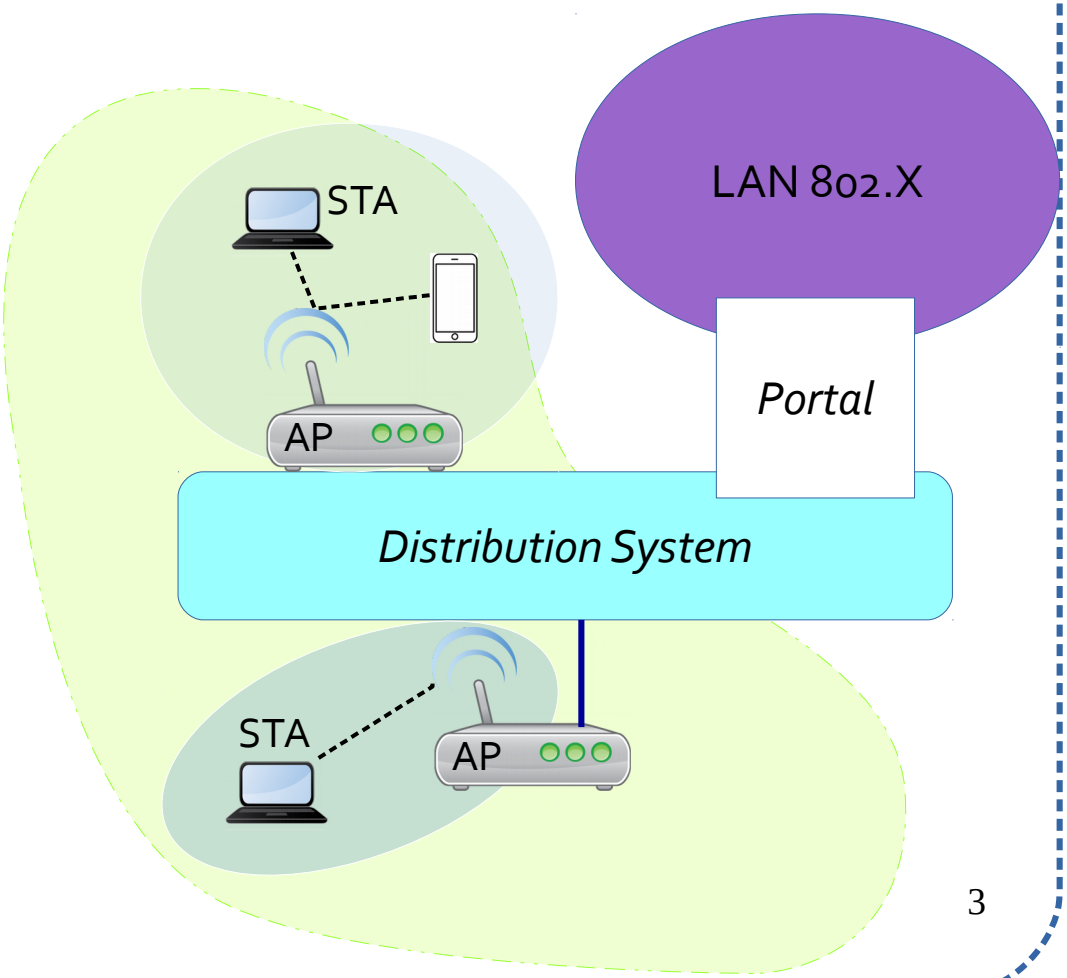
Standard IEEE 802.11

- Famille de standards définissant les spécifications de la couche physique et MAC d'un réseau local sans fil
- Modes de fonctionnement
  - Mode ad-hoc
    - Permet de construire des réseaux spontanés à couverture très réduite
    - Pas de protocole de routage défini dans la norme
    - Communication directe entre stations dans une zone réduite
    - ***Independent Basic Service Set*** **(IBSS)**
      - groupe de stations utilisant les mêmes fréquences radio et à portée radio les unes des autres
    - IEEE 802.11s

Mode infrastructure

Mode Infrastructure

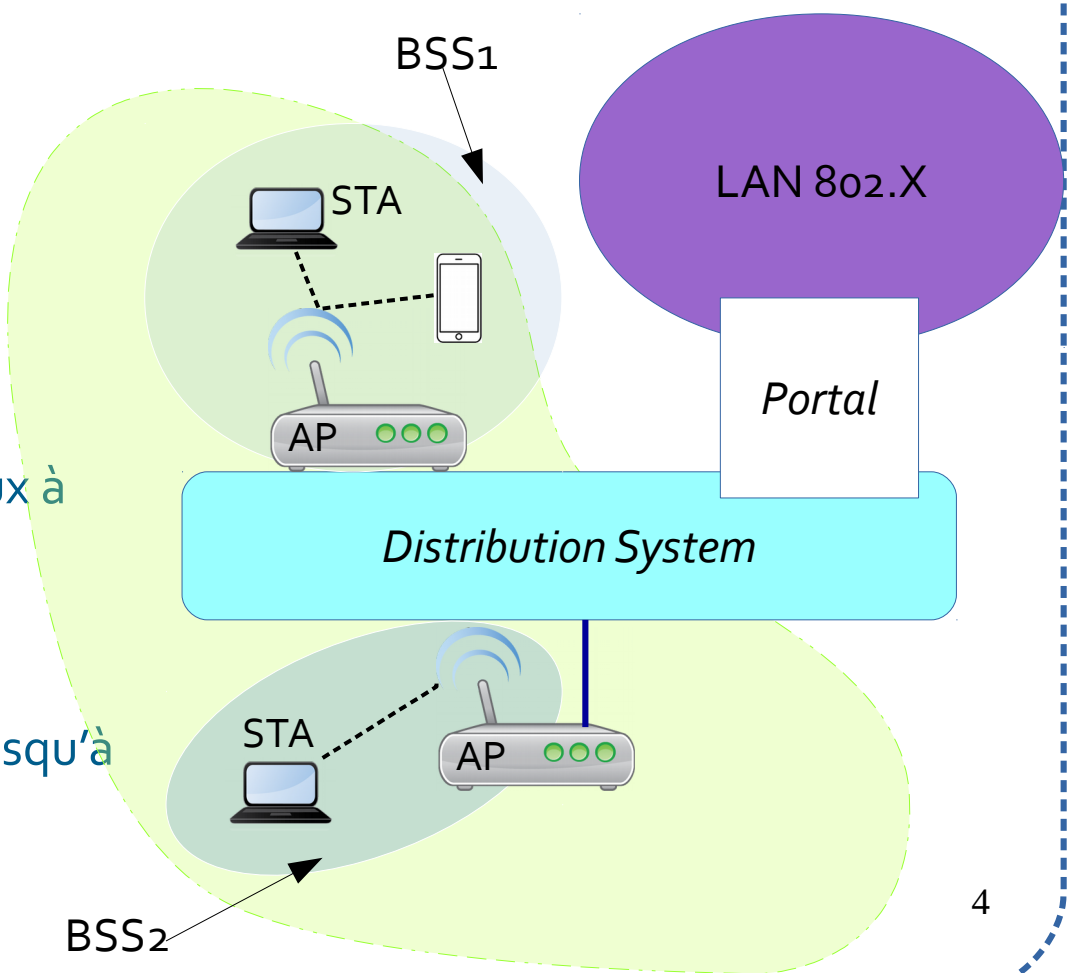
- Présence d'un point d'accès (*Access Point*, AP)
- Permet de compléter un réseau filaire existant en offrant un accès sans fil autour des points d'accès
- Nœud connecté à l'AP : station (STA)



Mode infrastructure : terminologie

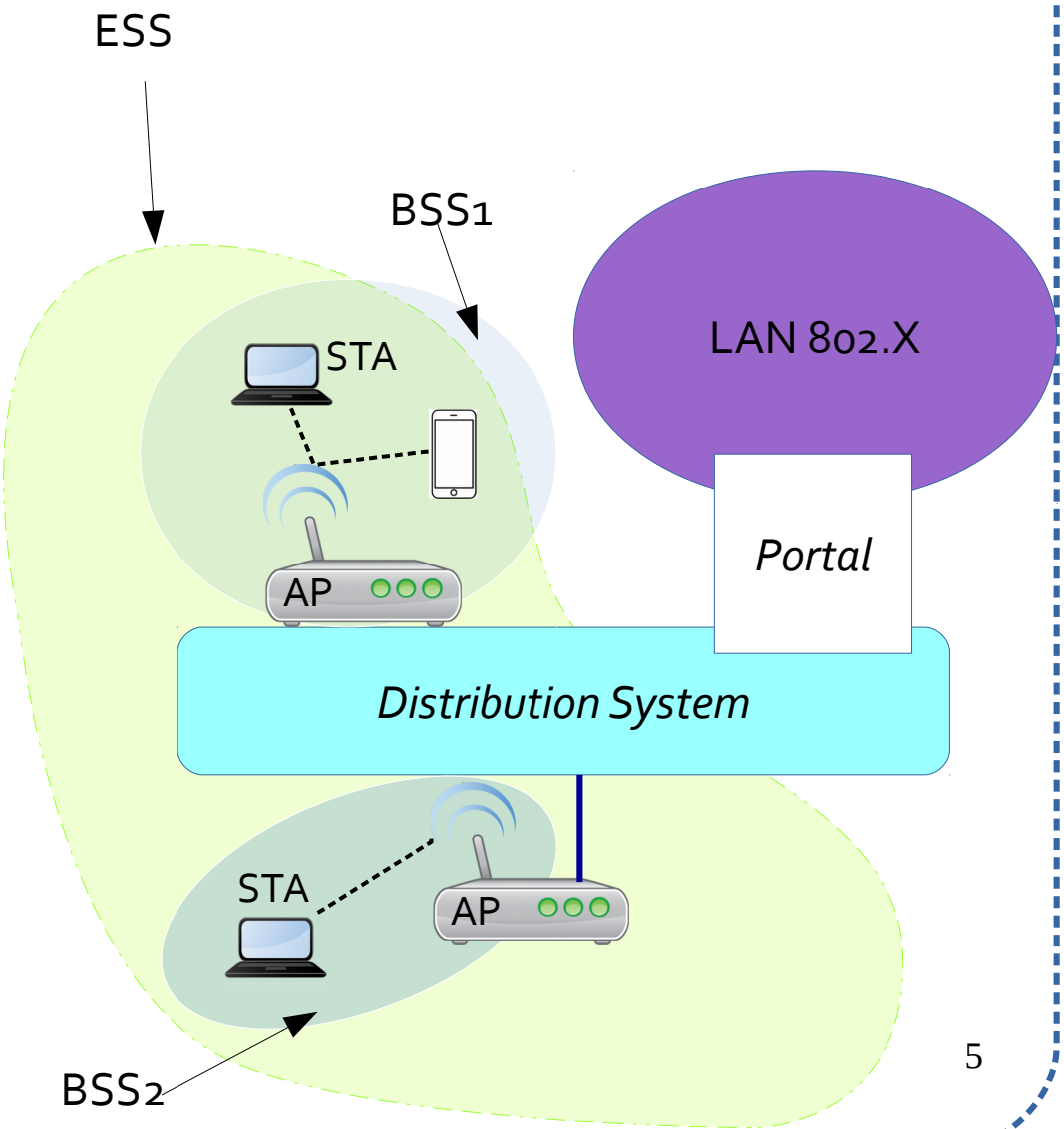
- Point d'accès (AP)
- Équipement central du mode infrastructure qui fédère autour de lui des terminaux sans fil à sa portée radio
- Généralement relié à un réseau filaire et supporte plusieurs fonctions
  - *handover*,
  - gestion énergie
  - …

- *Basic Service Set* (BSS)
  - Groupe de nœuds (1 AP et les terminaux à sa portée radio) utilisant les mêmes fréquences radio
- Dans un BSS, tout le trafic passe par l'AP
- Un BSS peut supporter théoriquement jusqu'à 100 stations
- **1 BSS = 1 cellule = 1 point d'accès**



Mode infrastructure : terminologie

- *Extended Service Set* (ESS)
  - **Regroupement de BSS**
  - Permet d'étendre la zone de couverture du réseau sans fil
  - Les communications entre stations de BSS différents, mais appartenant au même ESS, est effectué de manière transparente
    - Vision d'un même réseau pour les stations
    - Gestion du *handover* (*roaming* dans la terminologie 802.11)
- Ceci est rendu possible grâce à des fonctionnalités accrues au niveau de l'AP et au système de distribution qui assurent l'acheminement des trames



Mode infrastructure : terminologie

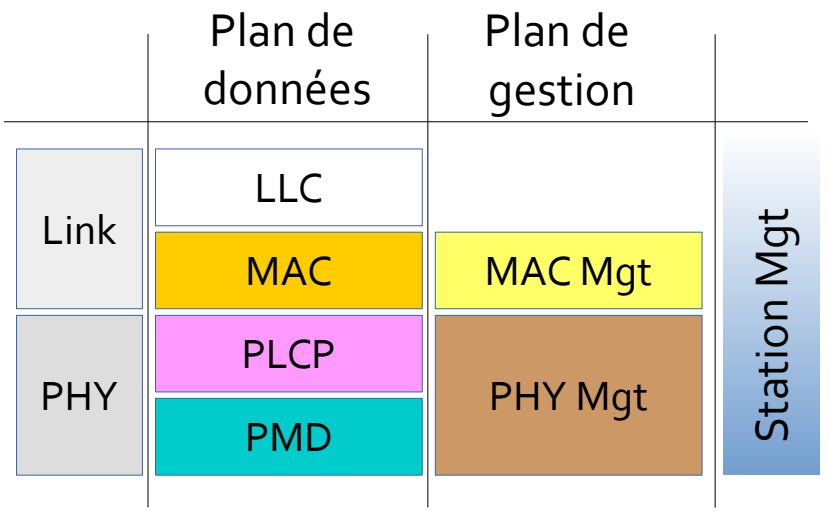
- *Distribution System* (DS)
  - **Interconnecte plusieurs BSS**
    - Par le biais des AP
    - Permet de former un unique réseau
  - Architecture protocolaire du DS non communiquée par IEEE 802.11
    - La norme définit par contre explicitement les services qu'il doit fournir

- *Portal*
  - équipement (pont) qui permet d'accéder à un réseau local 802.x
    - En général un réseau Ethernet

Services et fonctions 802.11

Architecture protocolaire

- MAC
  - Contrôle d'accès, fragmentation, chiffrement
- *MAC Management*
  - Synchronisation d'horloges, connexion au réseau, *handover*, gestion de l'énergie, *Message Information Base* (MIB)
- *Physical Layer Convergence Protocol* (PLCP)
  - Écoute de la porteurse
  - Adaptation des unités de données MAC à PMD
- *Physical Medium Dependent* (PMD)
  - Modulation et codage en ligne
- *PHY Management*
  - Sélection du canal de transmission, MIB
- *Station Management*
  - Coordination de toutes les fonctions de gestion



Services et fonctions 802.11

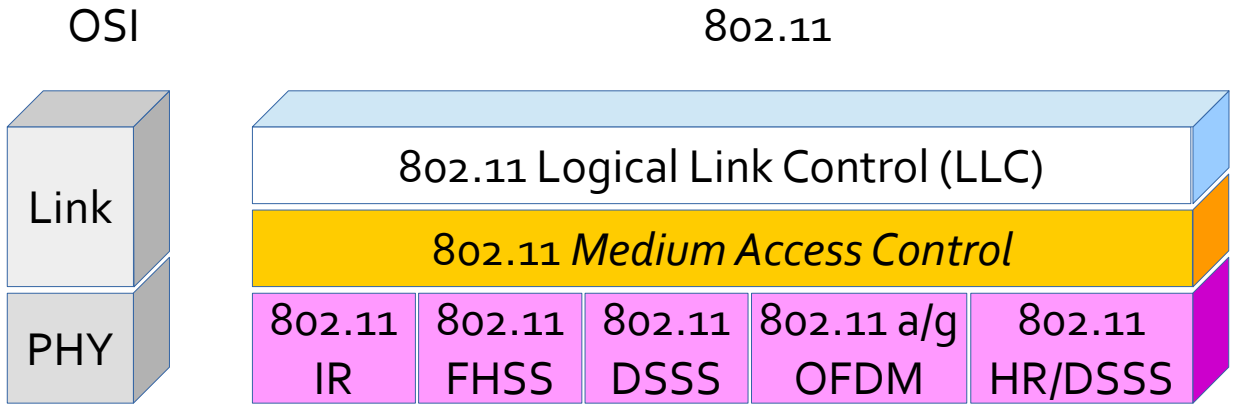
- Deux groupes de services
  - Services de base
    - ensemble de servies supportés par toute station 802.11
  - Services complémentaires
    - offerts par les point d'accès (valable pour le mode infrastructure)

- Services de base :
  - Services d'acheminement de trames : 2 types prévus
    - Service sans garantie (au mieux)
    - Service pour des données temps critique (optionnel)
  - Authentification / désauthentification :
    - Permet d'établir l'identité d'une station à une autre
  - Chiffrement des messages

Services et fonctions 802.11

- Services complémentaires (offerts par le point d'accès)
  - Association (connexion au réseau) / Dé-association
    - Une station qui souhaite intégrer un réseau sans fil avec infrastructure doit s'associer avec un AP
    - L'association permet à l'AP de connaître l'adresse de la station
      - utilisée par l'AP pour l'acheminement des trames
    - L'association intègre la station au BSS
    - Dé-association : service permettant de rompre cet attachement
  - Distribution
    - Permet d'aiguiller les trames dans le réseau
      - Si la destination est dans le même BSS, la trame est directement transmise sur le lien sans fil
      - Sinon, elle est transmise via le DS grâce au service intégration
  - Intégration
    - Permet à deux AP de communiquer au travers du DS

Famille des standards 802.11



- Deux bandes de fréquences utilisées
  - 2.4 Ghz pour 802.11 b/g
  - 5.1 Ghz pour 802.11 a
- Une troisième bande de fréquence (IR) est définie dans le standard mais il n'existe pas de produit commerciaux l'utilisant

Couche physique

Couche physique 802.11 : versions

- *Frequency Hopping Spread Spectrum* (FHSS)
  - 79 canaux de 1Mhz de largeur de bande
  - 3 ensembles de 26 séquences soit 78 séquences de sauts possibles
  - Modulation GFSK (*Gaussian shaped Frequency Shift Keying*) à 2/4 fréquences (1 ou 2 Mb/s)

- *Direct Sequence Spread Spectrum* (DSSS)
  - Modulation *Differential Binary Phase Shift Keying* (DBPSK) pour 1Mb/s
  - Modulation *Differential Quadrature* PSK (DQPSK) pour 2Mb/s

- Puissance maximale d'émission
  - 100 mW (Europe)
  - 1 W (USA)

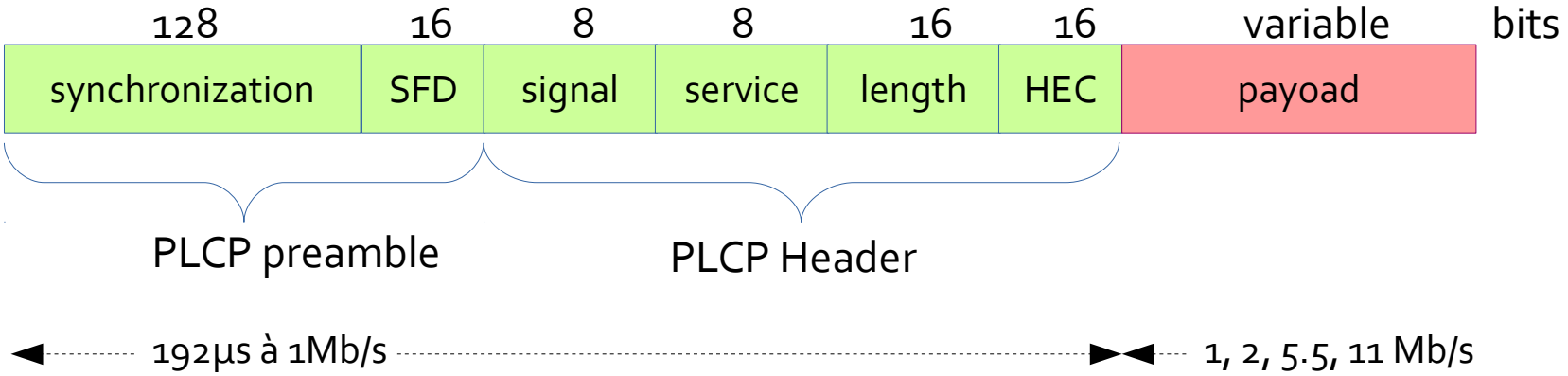
Couche physique 802.11b DSSS

- Solution la plus répandue actuellement même si la solution 802.11g prend de l'ampleur
- Canaux
  - Découpage en 14 canaux dont 13 sont utilisables en Europe
  - Les canaux recouvrant sont inexploitables simultanément
  - 3 canaux ont des intersections vides permettant de faire cohabiter 3 BSS avec peu de risque d'interférences

Couche physique 802.11b DSSS

- La sous couche physique PLCP
  - Adapte les unités de données MAC à la couche PMD
  - Indique à la sous-couche MAC si le medium est libre ou pas
    - *Clear Channel Assessment* (CCA)
  - Indique aux autres stations le débit d'émission avec lequel la trame de niveau MAC sera transmise
  - 2 formats de trames sont définis
    - format long
    - format court
    - Exemple pour le format Long

Couche physique 802.11b DSSS

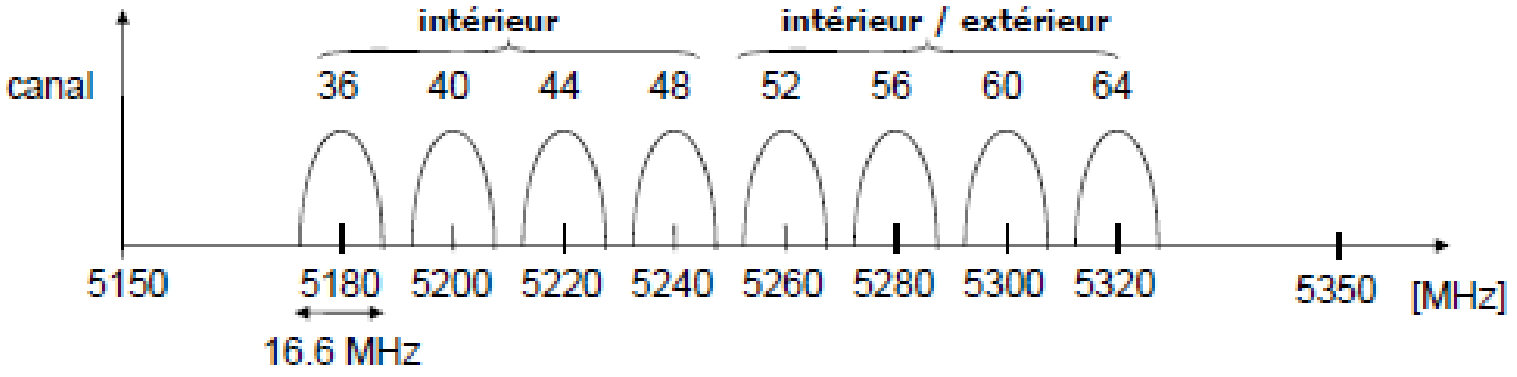


- *Synchronization* : 010101..
- *Start Frame Delimiter* (SFD) : 1111001110100000
- *Signal*
  - Débit de la charge utile (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK), ..
- *Service* : pour utilisation ultérieure, 00: conforme à 802.11
- *Length* : Taille de la charge utile
- *Header Error Check* (HEC)
  - protection des champs : *signal*, *service* et *length*
- **Remarque** : le *preamble* et *header* sont toujours transmis à 1Mbps

Couche physique 802.11a OFDM

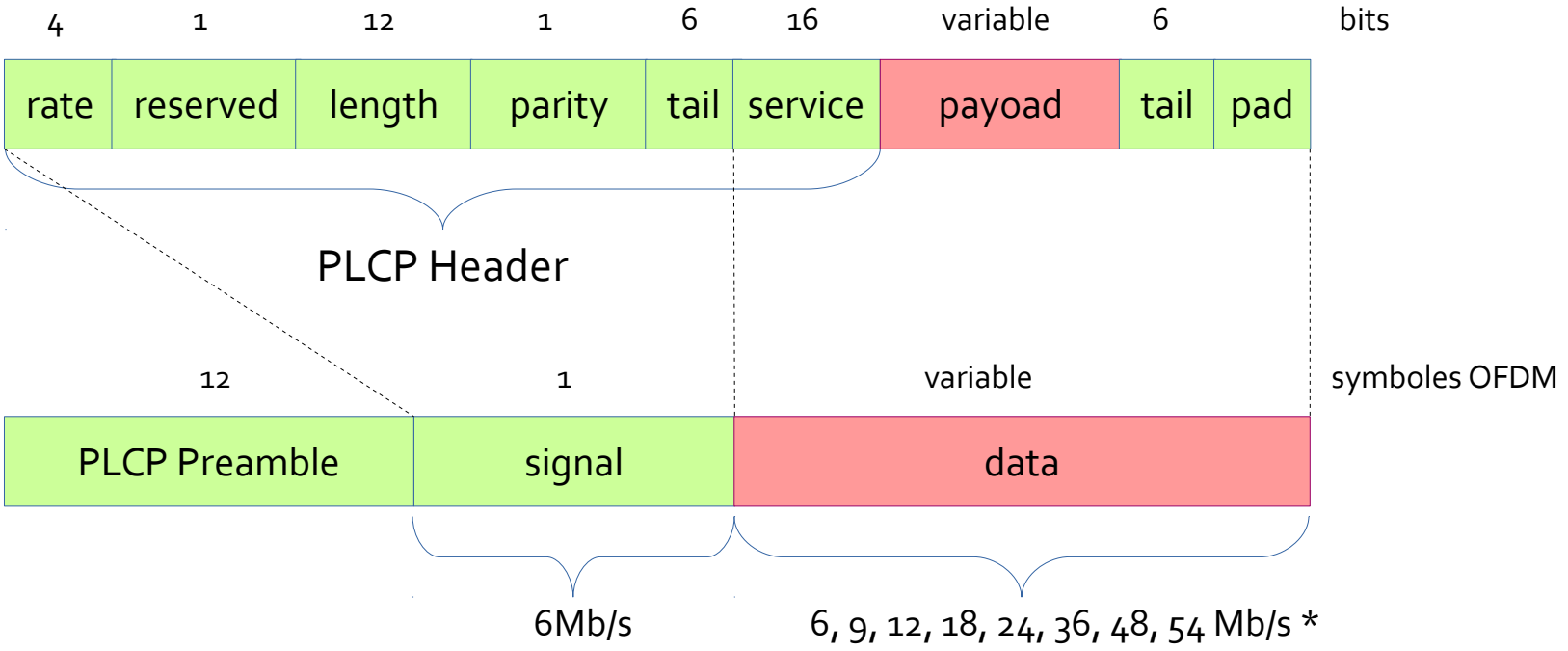
- Canaux
  - 8 canaux de 20 Mhz sont séparés
  - Chaque canal contient 52 sous canaux de 300Khz utilisables en parallèle
  - Débits de 6 à 54Mb/s
    - Modulation BPSK: 0,125 Mb/s par sous canal → 6Mb/s
    - Modulation QAM84: 1,124 Mb/s par sous canal → 54Mb/s

Fréquence médiane = 5180 + 20*numéro de canal [MHz]



Couche physique 802.11a OFDM

La sous couche PLCP
– Même principe que pour 802.11b



* : Pour un espacement inter-canal de 20MHz (autres valeurs d'espacement possibles : 10MHz et 5MHz). Débits obligatoires : 6, 12 et 24Mb/s. Valeur spécifié par le champ signal

Sous-couche MAC

MAC 802.11

- Fonctions MAC de 802.11 détaillées ci-dessous :
  - Contrôle d'accès au canal
  - Adressage
  - Fragmentation
  - Synchronisation
  - Connexion au réseau/point d'accès
    - Processus de sondage (*probing*)
    - Processus d'authentification
    - Processus d'association
  - Gestion du *handover*
  - Gestion d'énergie

Plan de données

Plan de gestion

MAC 802.11 : contrôle d'accès au canal

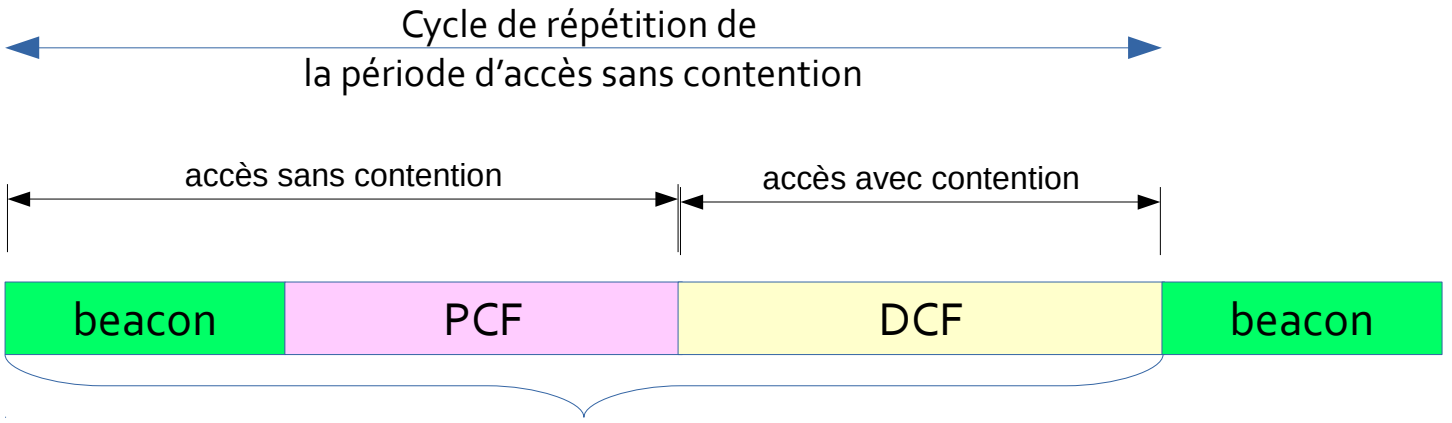
- Deux types de service de communication de niveau MAC
  - Service d'acheminement *Best effort*, i.e. sans garantie :
    - Service avec contention
    - Avec possibilité de diffusion et diffusion limitée (multicast)
  - Service d'acheminement pour données critiques, supposé offrir des garanties sur les délais et débits (optionnel)
    - Service sans contention

- Pour cela, deux modes d'accès sont définis
  - *Distributed coordination function* (DCF)
  - *Point coordination function* (PCF) (optionnel)

- Ces deux modes d'accès sont exécutés cycliquement

MAC 802.11 : contrôle d'accès au canal

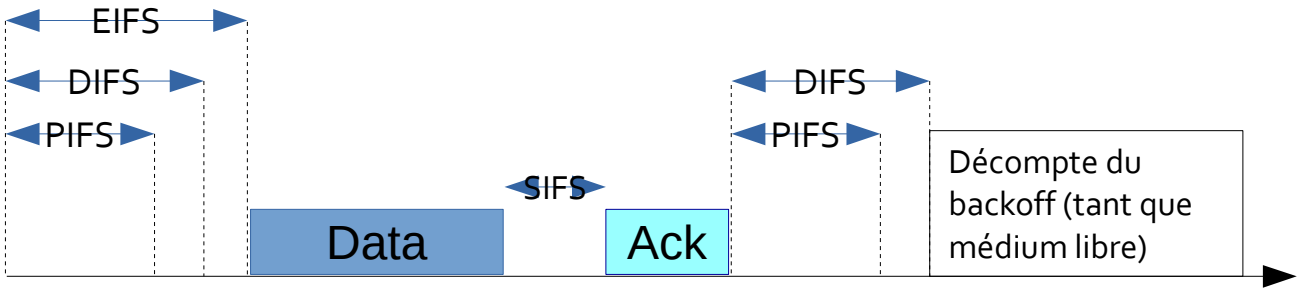
Structure temporelle



- Beacon
  - Trame de gestion
  - Transmission quasi périodique
- PCF et DCF
  - Échange de plusieurs trames avec garanties différentes
  - Échange unicast : trame de données suivie d'une trame d'acquittement

MAC 802.11 : espaces inter-trames

- Pour réglementer les échanges entre trames de contrôle et de données et entre échanges en mode PCF et en mode DCF, plusieurs espaces inter-trames (*InterFrame Spacing*) sont définis, parmi lesquels :
  - SIFS (*Short* IFS): pour les échanges atomiques
  - PIFS (PCF IFS): pour donner la priorité à un accès PCF sur DCF
  - DIFS (DCF IFS): pour accès normal en mode DCF
  - EIFS (*Extended* IFS): à utiliser à la place du DIFS lors d'une tentative d'accès suite à la détection d'une erreur de trame
  - **SIFS < PIFS < DIFS < EIFS**



MAC 802.11 : espaces inter-trames

MAC 802.11 : espaces inter-trames

- Valeurs des différents IFS dépendent de la couche physique
  - Ils sont exprimés en unités de « slot time » (comme dans Dix Ethernet)
  - **SIFS** et ***slot time*** sont explicitement spécifiés par la couche physique des différents standards 802.11, les autres sont déduits
    - **PIFS = SIFS + Slot_Time**
    - **DIFS = SIFS + 2·Slot_Time**
    - **EIFS = SIFS + DIFS + temps de transmission de ACK au débit de** 1Mbps

	802.11	802.11b	802.11a	802.11g
Slot time (µs)	50	20	9	9
SIFS (µs)	28	10	16	10/20

Mode *Distributed Coordination Function* (DCF)

- Technique d'accès pour le mode avec infrastructure et mode ad-hoc basée sur la technique CSMA/CA
  - Accès aléatoire suivant la méthode CSMA (écouter avant de transmettre)
    - Écoute pendant une durée fixe **DIFS** pour s'assurer que le canal est libre
    - Fonction écoute appelée ***Clear Channel Assessment*** **(CCA)**
      - Comparaison de la puissance de réception à un seuil (-82 dbm) + éventuellement (fonction du constructeur)
      - Détection du préambule de la trame physique 802.11
      - ***Network Allocation Vector*** (NAV) appelé aussi le *virtual carrier sensing* : fonction de **réservation du canal** pour une durée spécifiée dans une trame 802.11

Mode DCF

- Pas de possibilité de détecter de collision
  - Phénomène d'éblouissement : puissance d'émission >> puissance de réception. Récupération du signal reçu compliquée !

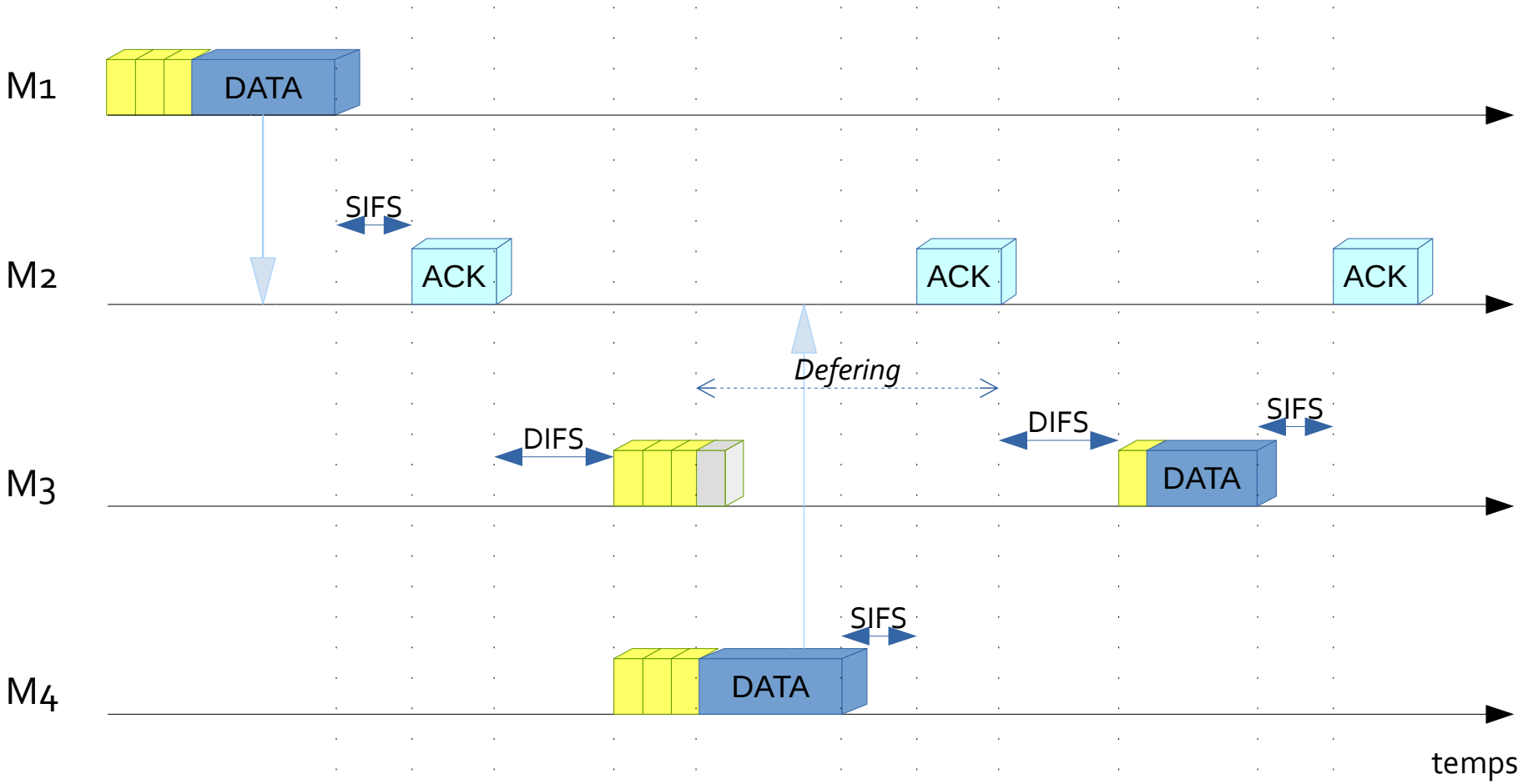
- **Détection de collision indirecte** par non réception d'acquittement
  - Acquittement systématique des trames émises

- **Évitement de collision** (*Collision Avoidance* (CA)) dont le rôle est de réduire la probabilité des collisions
  - Procédure de ***Backoff***

Mode DCF

- La procédure de *Backoff*
  - Attendre que le canal reste libre pendant DIFS
  - La station continue à écouter le bus pendant une durée de temps aléatoire additionnelle appelée *backoff time* (temps de *backoff*);
  - Le *backoff time* est tiré aléatoirement sur l'intervalle [0, CW]
  - *Contention Window* (CW) exprimée en unités de *slot time*
    - Initialisée après chaque transmission réussie à CW_{min}
    - CW_{min} est fixée par le standard
      - 7 pour 802.11
      - 15 pour 802.11a/g
      - 31 pour 802.11b
  - **SI** le canal reste libre durant le *backoff* la station peut accéder au canal
  - **SINON** dès que le canal est occupé, le compteur du *backoff* est arrêté
    - Le décompte ne peut reprendre que lorsque le canal reste libre pendant DIFS: on parle de *defering*

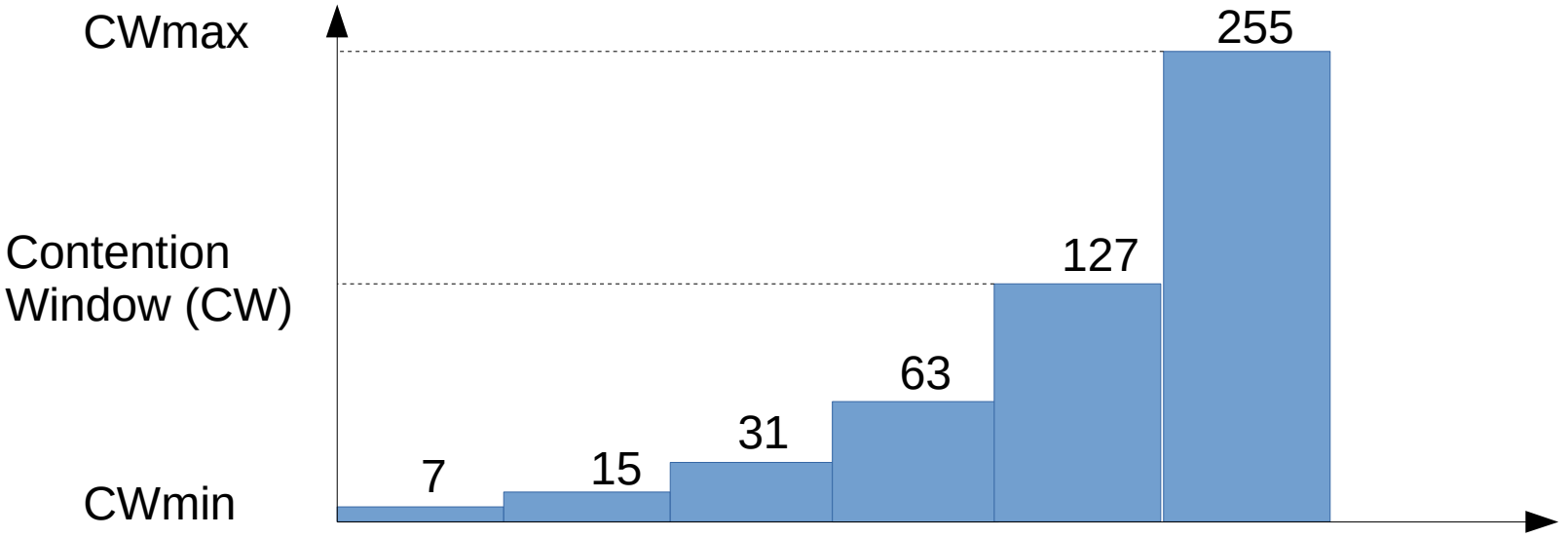
Mode DCF



: *slots* de *backoff*

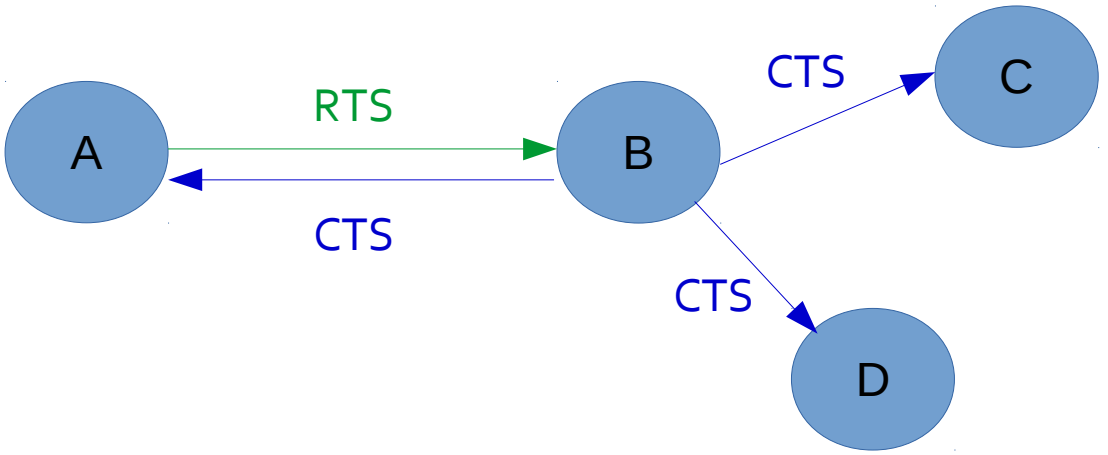
Mode DCF

- Après transmission de trame
  - Si la transmission échoue (i.e. pas d'ACK) on double la fenêtre de *backoff* (on parle de *Backoff* exponentiel)
    - CW=min{2*CW+1, CW_{max}}
    - CW_{max} est fixé dans la norme
      - 255 dans 802.11
      - 1023 dans 802.11 a/b/g

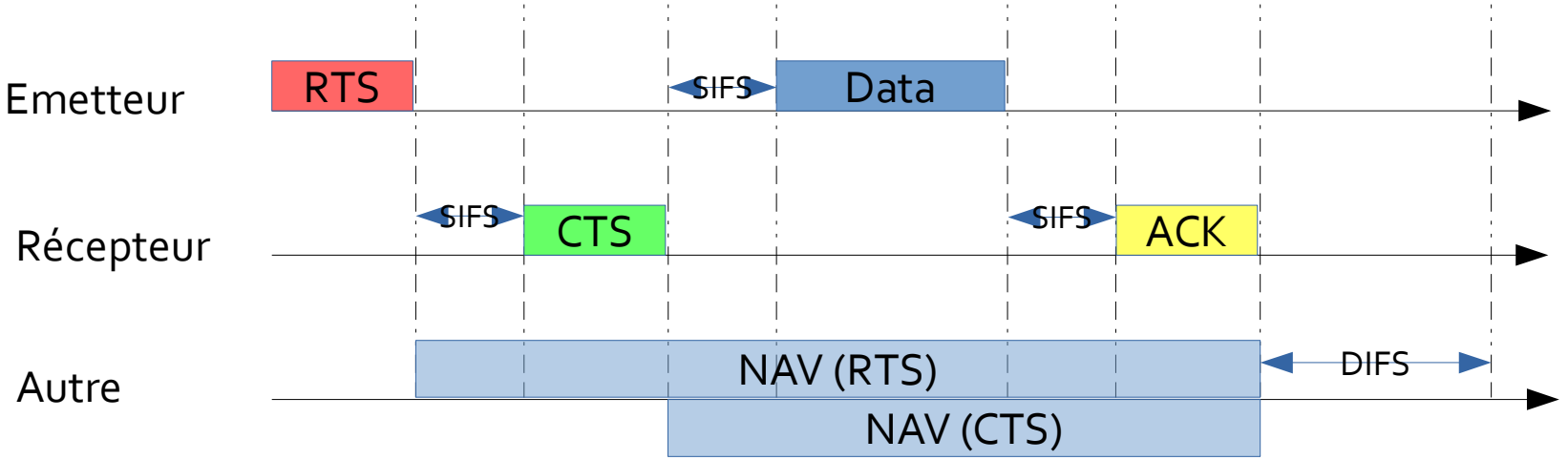


Mode DCF

- La réservation de ressources avec RTS/CTS
  - *Request To Send* (RTS) émis avant de démarrer la communication par l'émetteur
  - *Clear To Send* (CTS) envoyé en réponse par le récepteur à destination de l'émetteur ainsi qu'à tous les voisins du récepteurs
    - Les nœuds voisins savent ainsi qu'une communication va avoir lieu et n'essaient pas de communiquer avec le récepteur pendant la durée de la transmission



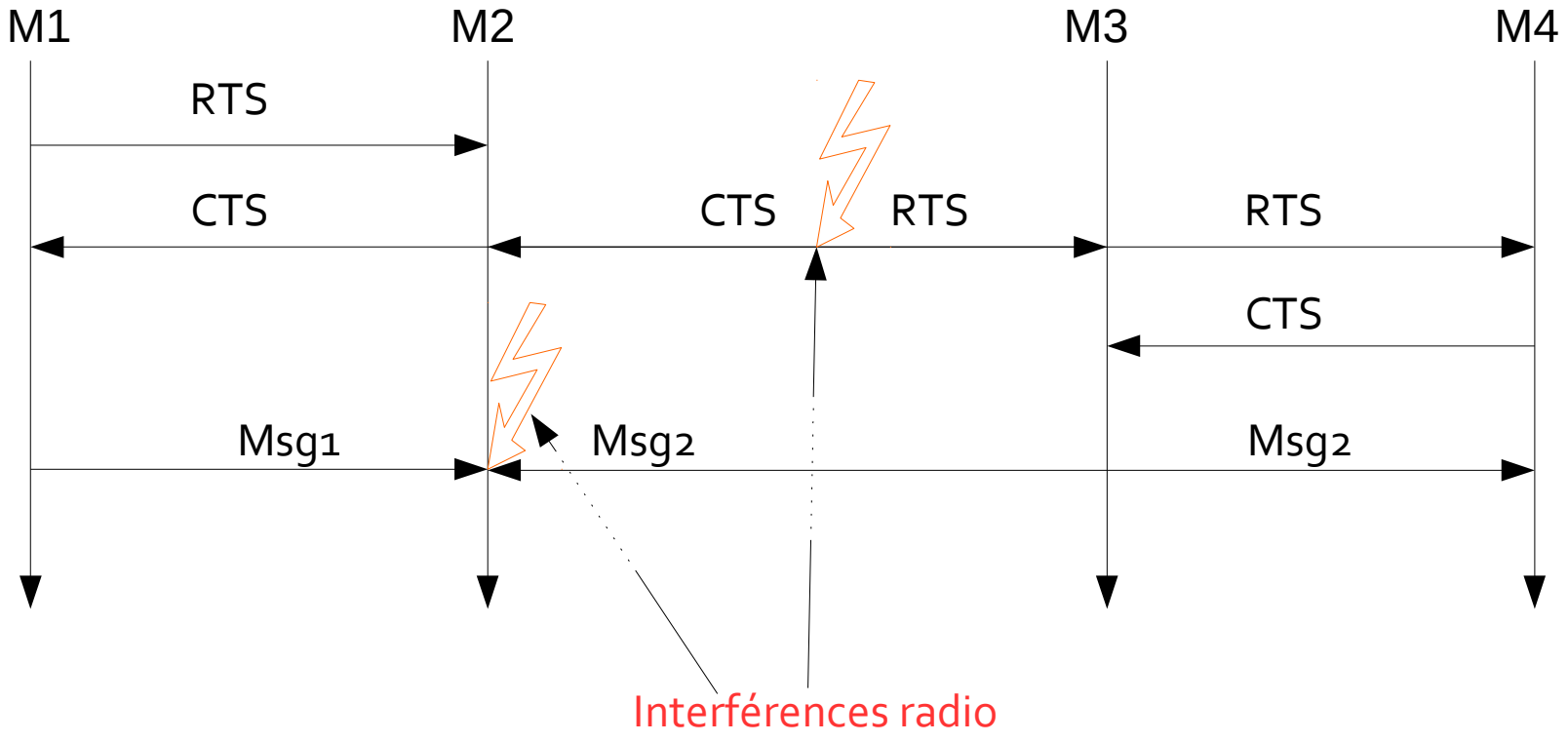
Mode DCF



- IFS et Atomicité
- Attente des nœuds à portée
  - À portée du RTS
  - A portée du CTS

Mode DCF

- Le mécanisme RTS / CTS permet d'éviter certaines situations de terminaux cachés mais ne garantit pas qu'il n'y en aura jamais
  - Certaines situations problématiques peuvent encore survenir



Mode DCF

- Avantages du mode RTS/CTS
  - Adapté au problème du nœud caché
  - Efficace en cas de surcharge du réseau
    - RTS trame courte => protocole plus réactif en cas de collisions entre trames RTS
- Inconvénients
  - Débits réduits à cause du trafic supplémentaire introduit
  - Ne peut être appliqué au trafic *broadcast/multicast*

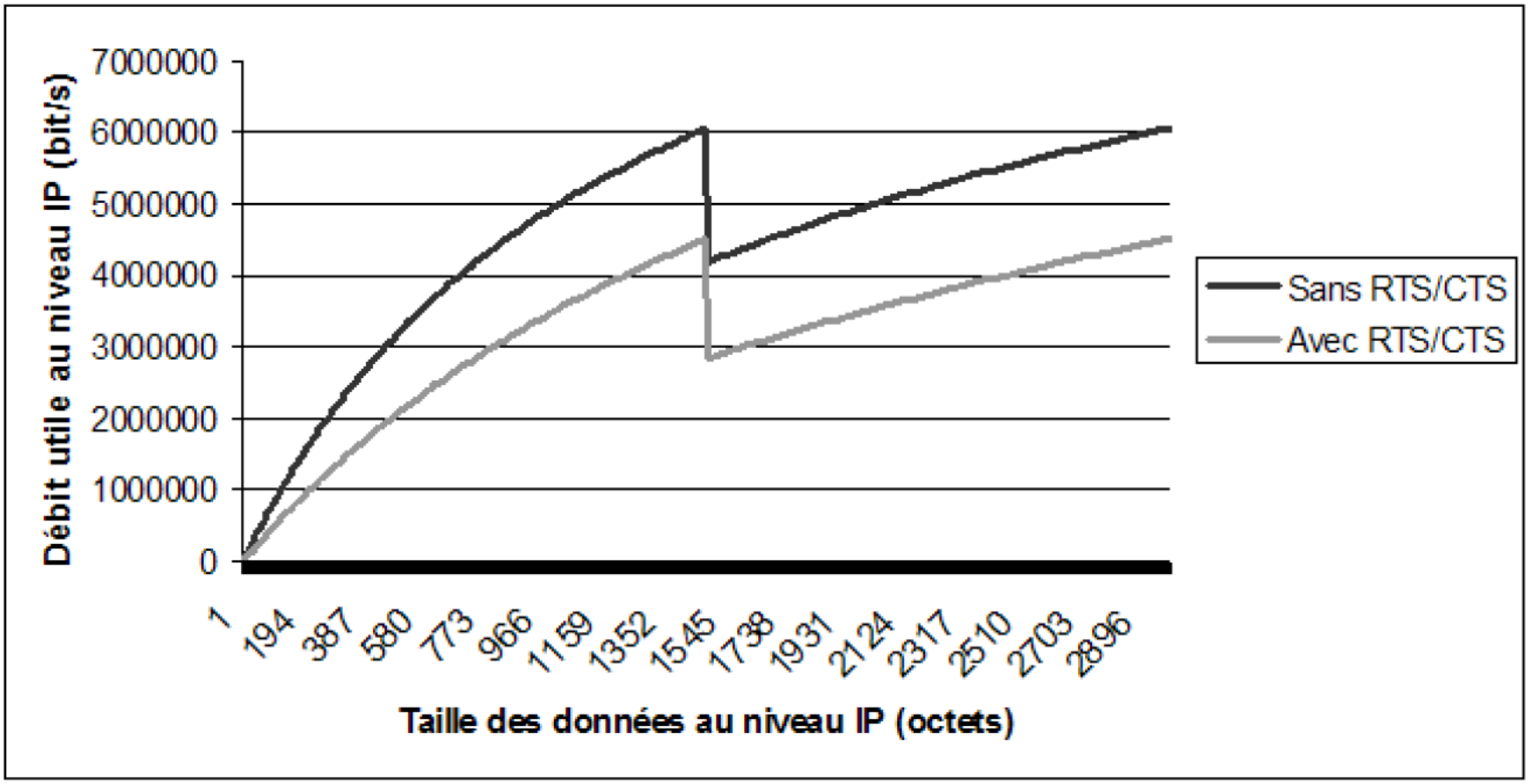
- En pratique
  - Option peu utilisée
  - Si utilisée, activée lorsque la taille de la trame dépasse un certain seuil fixé par un paramètre protocolaire
    - *RTS-Threshold* (pouvant être configuré sur l'équipement)
    - Utilisée uniquement avant l'envoi de la première trame en cas de fragmentation

Mode DCF

- Le mécanisme d'écoute virtuelle du médium ou ***Network Allocation Vector*** **(NAV)**
  - Chaque station maintient une estimation de la durée pendant laquelle le canal va être alloué à une autre station
    - Permet de différer ses tentatives d'accès au support.
  - Cette durée est annoncée dans les trames de données ainsi que par les trames RTS/CTS (champ d'en-tête prévu)
    - Pour une trame de données: durée depuis la transmission de la trame de donnée jusqu'à la fin de transmission de l'acquittement
    - Dans RTS/CTS: tient compte de toute la transaction
      - Transmissions RTS, CTS, Data, ACK
  - Les stations n'actualisent leur NAV que lorsque la valeur de la durée qu'ils viennent de recevoir dépasse celle qu'ils possèdent déjà

Mode DCF

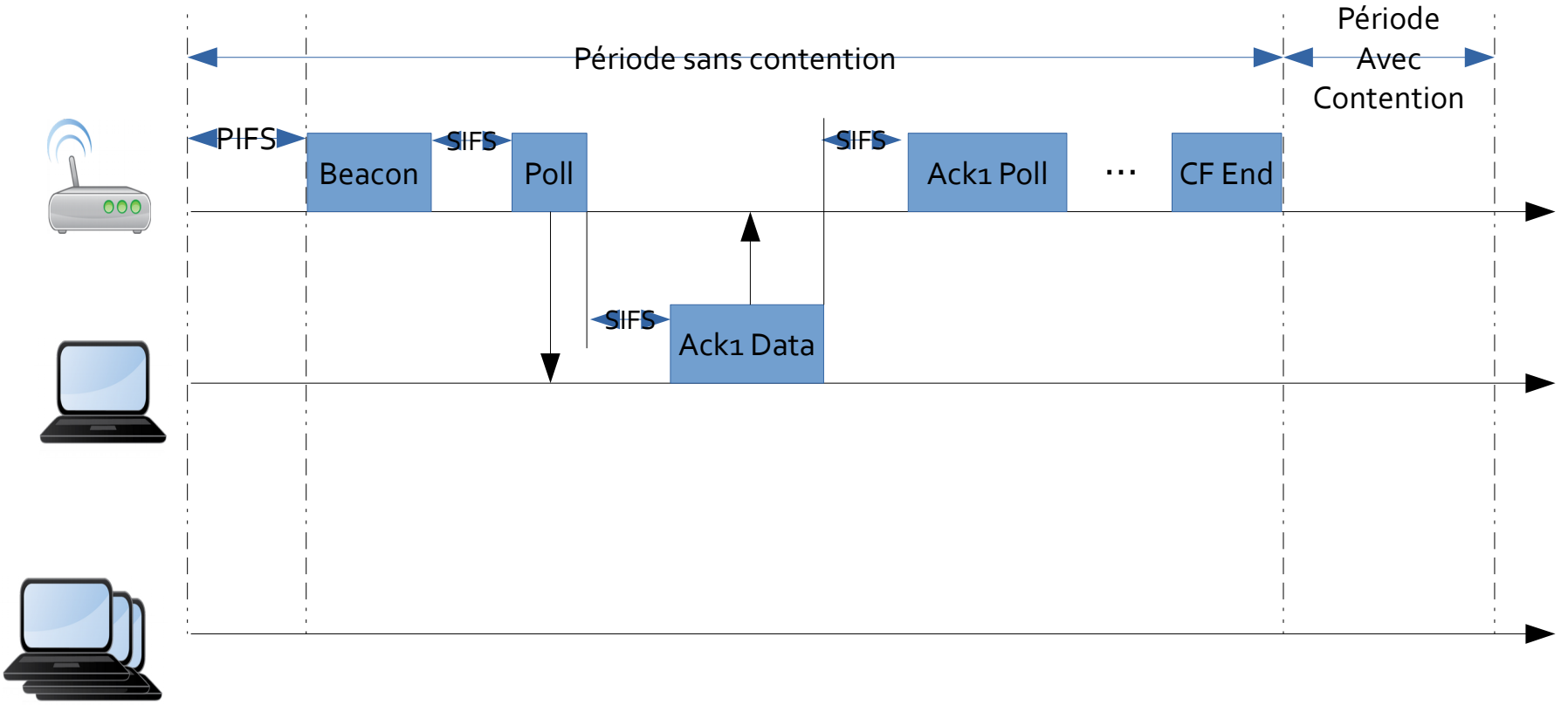
- Impact sur le débit utile au niveau IP
  - Exemple pour un lien 802.11b à 11Mb/s



Mode *Point Coordination Function* (PCF)

- *Point Coordination Function*
  - Possible uniquement en mode infrastructure
  - Proposé pour les applications avec contraintes sur délai de transfert et débit
  - L'AP prend le contrôle des transmissions en choisissant les stations qui peuvent émettre: ***polling***
    - Chaque interrogation de station donne lieu à une et une seule transmission
    - Algorithme de *polling* non défini par le standard

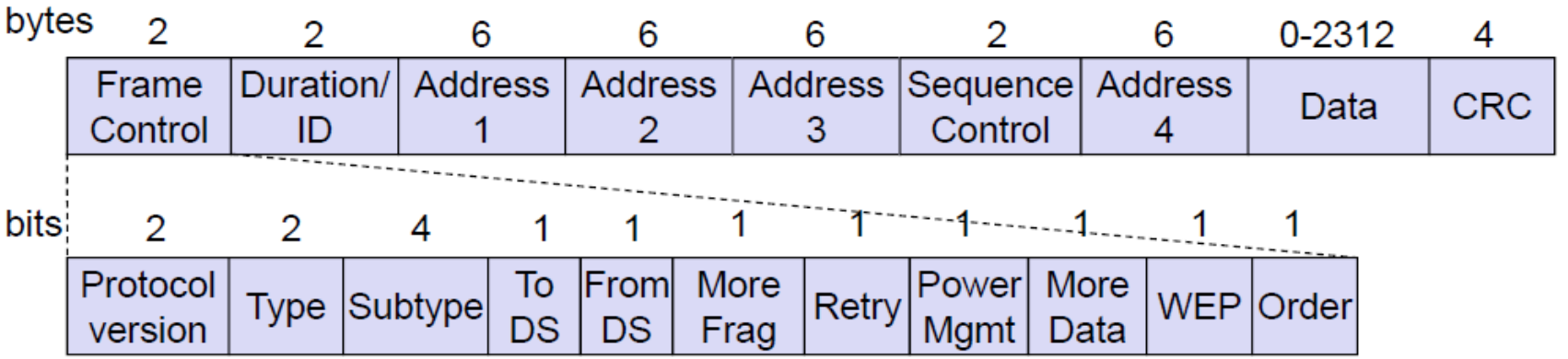
Mode PCF



- Prise de parole par l'AP
- Transmissions séparées de SIFS
  - Pas de réponse après SIFS : rien à émettre par la STA

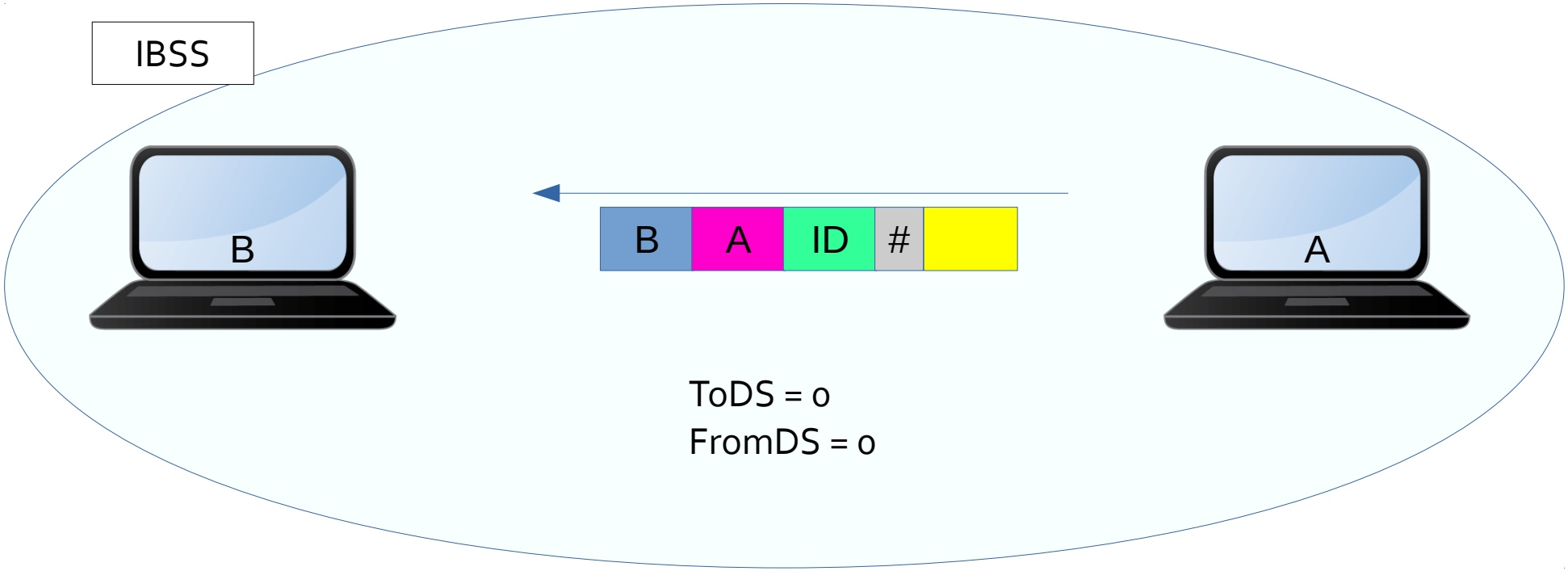
Format de trames

- Les trames 802.11
  - Différents types de trames:
    - Trames de contrôle
    - Trames de données
    - Trame de gestion
  - Particularités :
    - Numéro de séquence : nécessaire contre la duplication des trames à la suite de la perte de l'acquittement
    - 4 champs d'adresse : La sémantique des @1, .. @4 est dépendante des valeurs des champs *ToDS*, *FromDS*
    - Divers : durée de transmission, gestion de l'énergie, ..



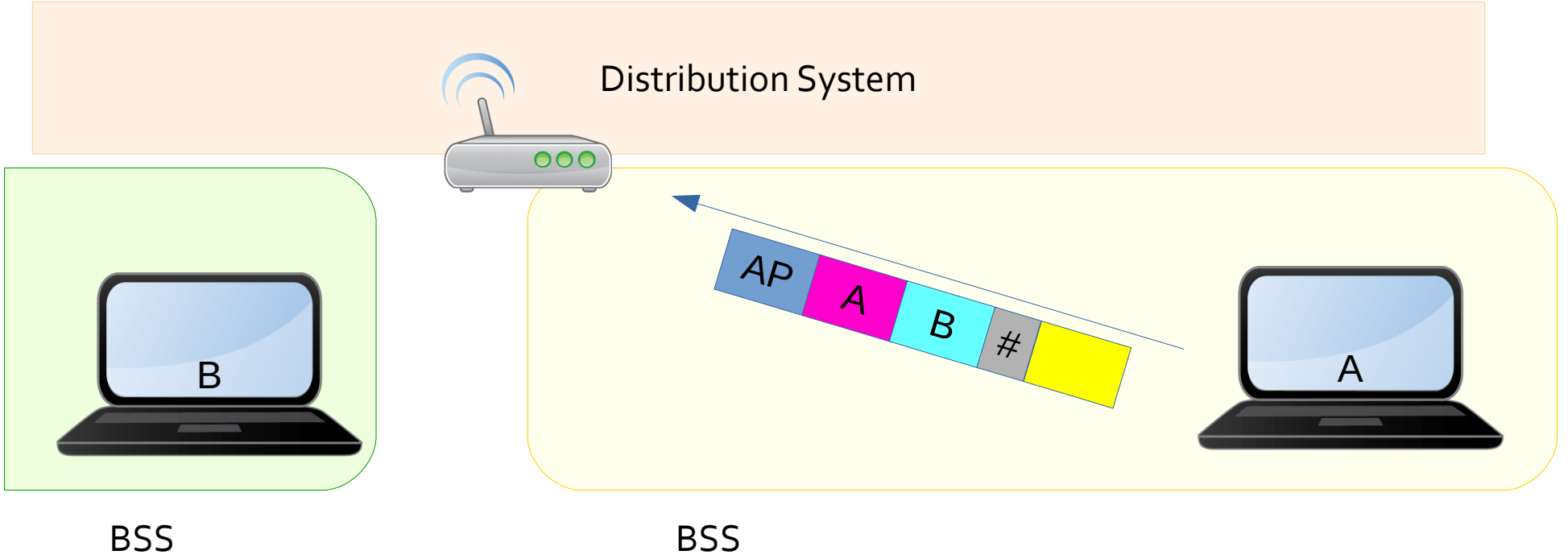
Format de trames : adressage

- Illustration de l'utilisation des champs adresses
  - Pour les réseaux ad-hoc



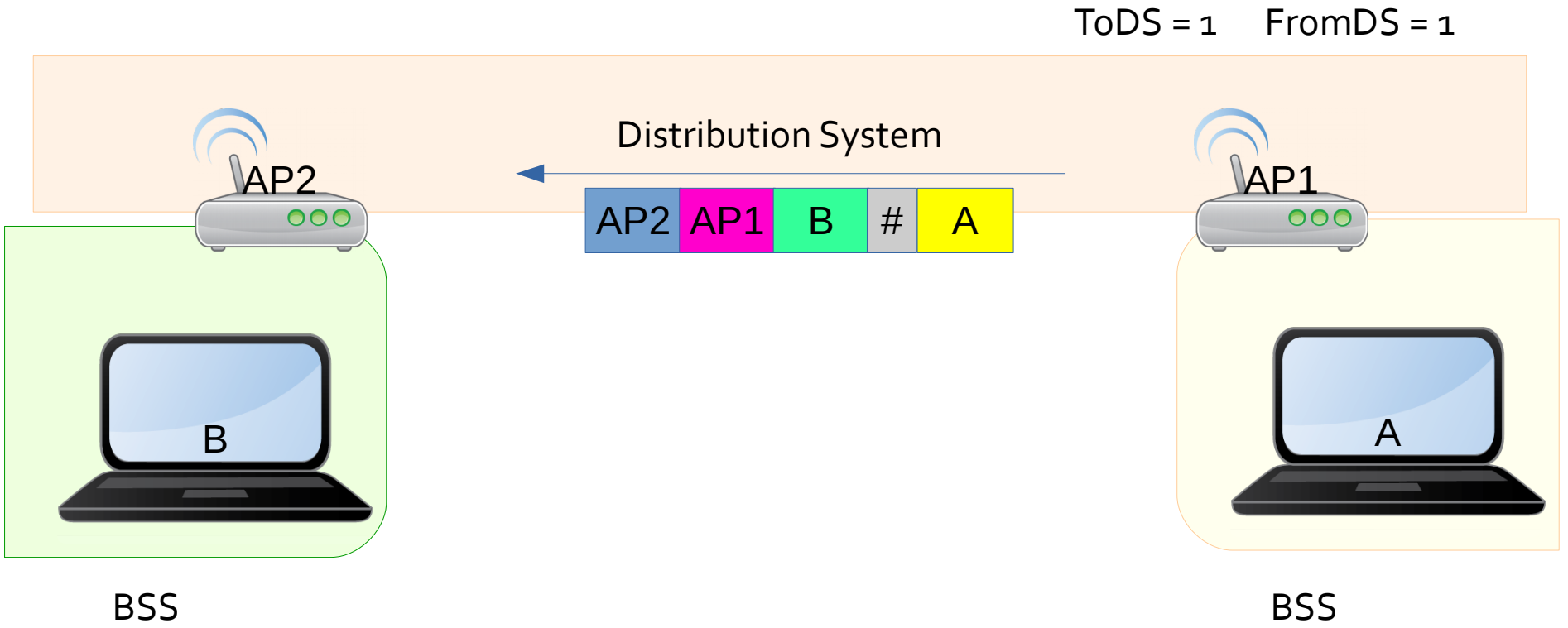
Format de trames : adressage

- Réseau avec infrastructure: transmission dans le DS



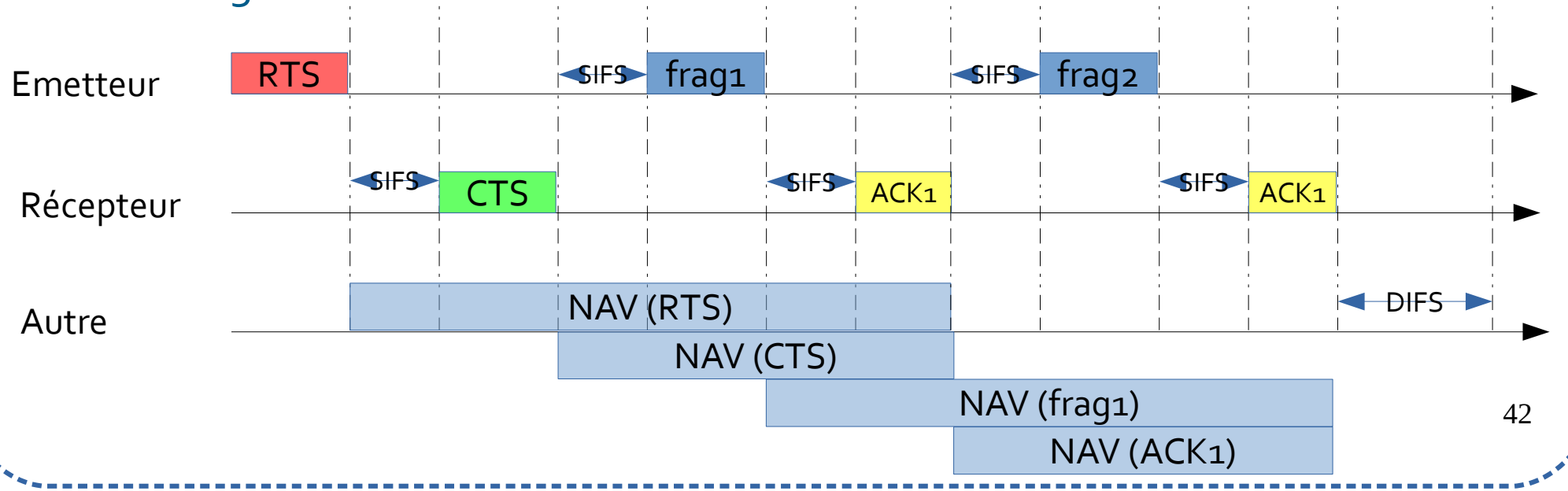
Format de trames : adressage

- Réseau avec infrastructure: transmission vers l'AP



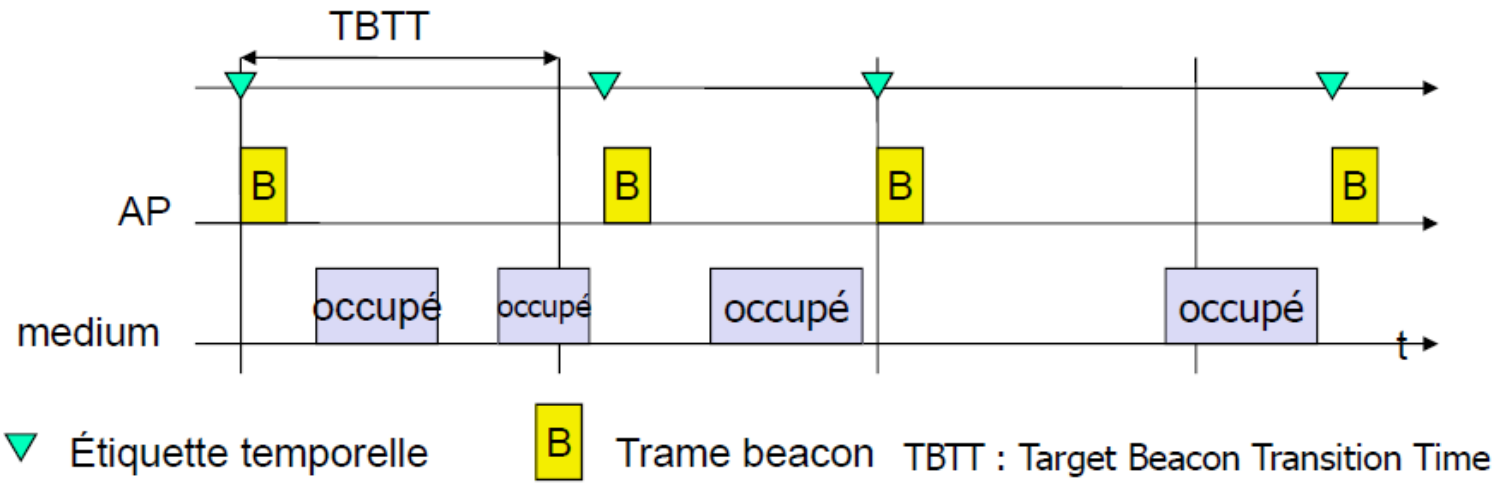
MAC et fragmentation

- Gestion de la fragmentation
  - La couche MAC 802.11 divise un MSDU (Mac SDU) trop grand en plusieurs fragments qui sont transmis individuellement
- Méthodologie
  - Transmission du MSDU est **atomique**
    - Chaque fragment est acquitté en ligne
  - Numérotation des fragments
  - En cas de non acquittement d'un fragment, retransmission instantanée du fragment



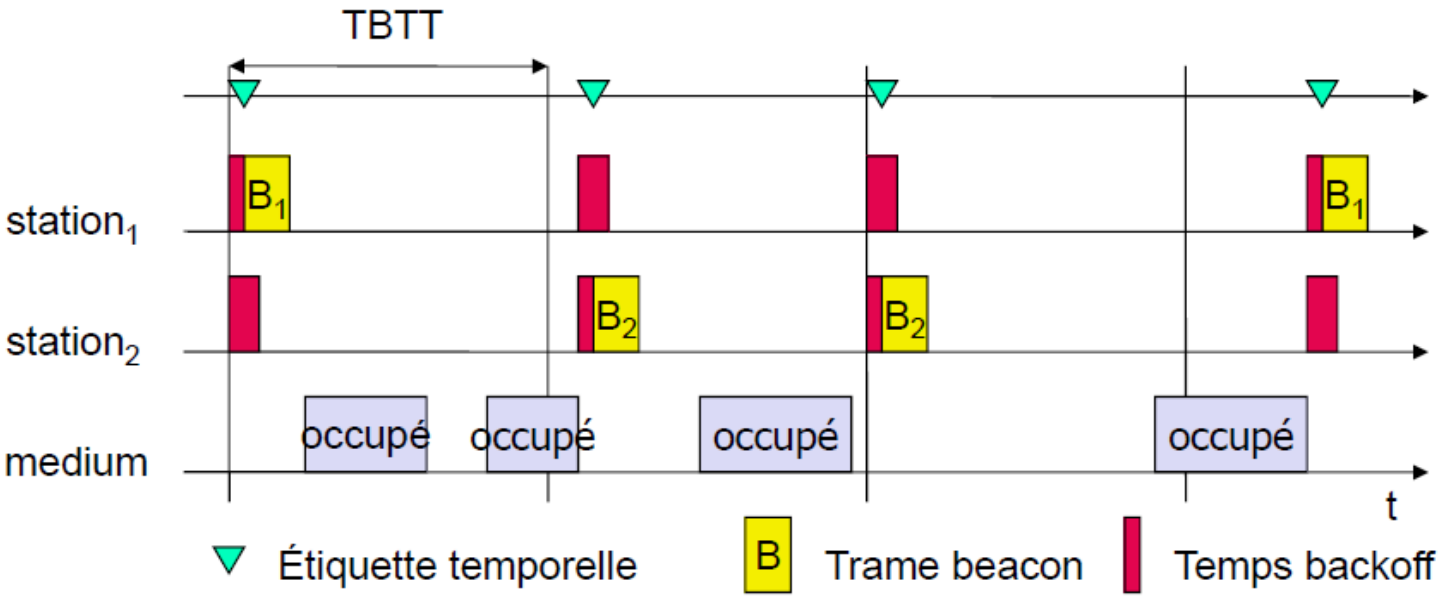
MAC et synchronisation

- Synchronisation des horloges des stations
  - Nécessaire pour assurer plusieurs fonctions :
    - Localiser le début du Mode PCF, Gestion de l'énergie, fixer les instants de sauts avec une couche physique type FHSS
  - Comment ? Synchronisation avec la trame *beacon* comportant une étiquette temporelle
  - En mode avec infrastructure : étiquette = valeur de l'horloge de l'AP



MAC et synchronisation

- En mode ad-hoc, chaque noeud essaye d'imposer la valeur de son horloge



TBTT : Target Beacon Transition Time

MAC et connexion à l'AP

- Connexion à l'AP en trois phases :
  - Sondage de l'environnement (*Scan*)
  - Authentification
  - Association
- La phase de sondage peut être de deux types
  - *Scan* passif
    - La station passe de canal en canal et stocke les trames *beacon* qu'elle reçoit
  - *Scan* actif
    - La station envoie une trame de *probe* sur chacun des canaux et attend une trame réponse
- Lorsque la station peut se joindre à plusieurs BSS
  - Dans ce cas, elle peut décider de se joindre à celui qui offre le signal le plus puissant
  - C'est typiquement le cas lorsqu'une station se déplace

MAC et connexion à l'AP

- La phase d'authentification :
  - Une fois un BSS choisi, la station s'authentifie auprès de l'AP
  - Permet de s'assurer que la station a le droit d'accéder au réseau sans fil
  - L'authentification peut
    - N'impliquer aucun contrôle (système ouvert) (définie dans le standard 802.11)
    - être basée sur l'identifiant du BSS/ESS
    - être basée sur l'adresse MAC
    - être basée sur la connaissance d'une clé partagée (définie par le standard 802.11)
    - être basée sur une architecture d'authentification plus complexe (extension du standard)

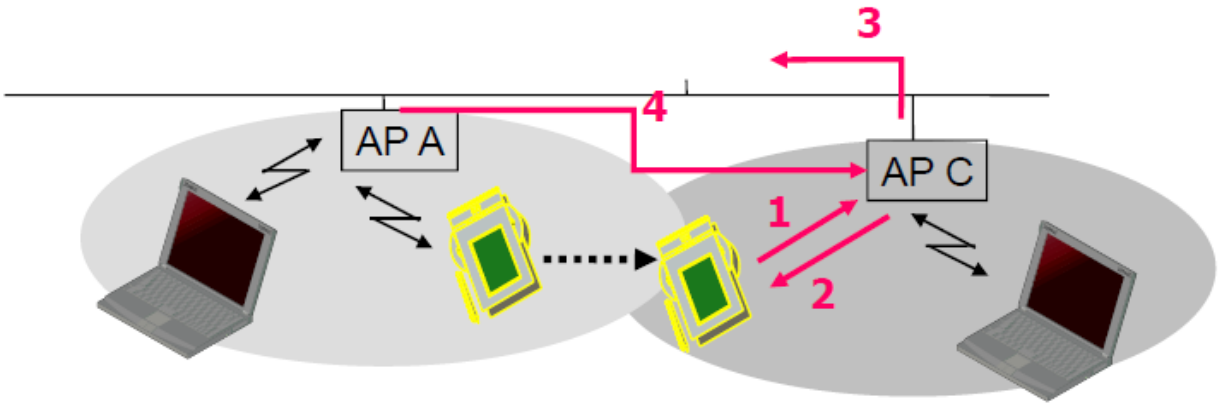
MAC et connexion à l'AP

- La phase d'association
  - Requête d'association suivie d'une réponse d'association
  - Permet d'intégrer la station dans le BSS et d'échanger des paramètres protocolaires
    - TBTT
  - Liste des débits qui doivent être supportés par la station pour se joindre au BSS
  - …

MAC et *handover*

- Le handover transparent
  - Prenons un terminal T associé à l'AP A et souhaitant rejoindre l'AP C

1) Requête de ré-association avec l'AP C
2) AP C confirme l'association et intègre le terminal dans son BSS
3) AP C diffuse sur le système de distribution l'adresse de T comme étant un terminal qui lui est associé
4) AP A fait suivre à AP C les trames qui ne lui ont pas encore été envoyées et dé-associe le terminal de son BSS



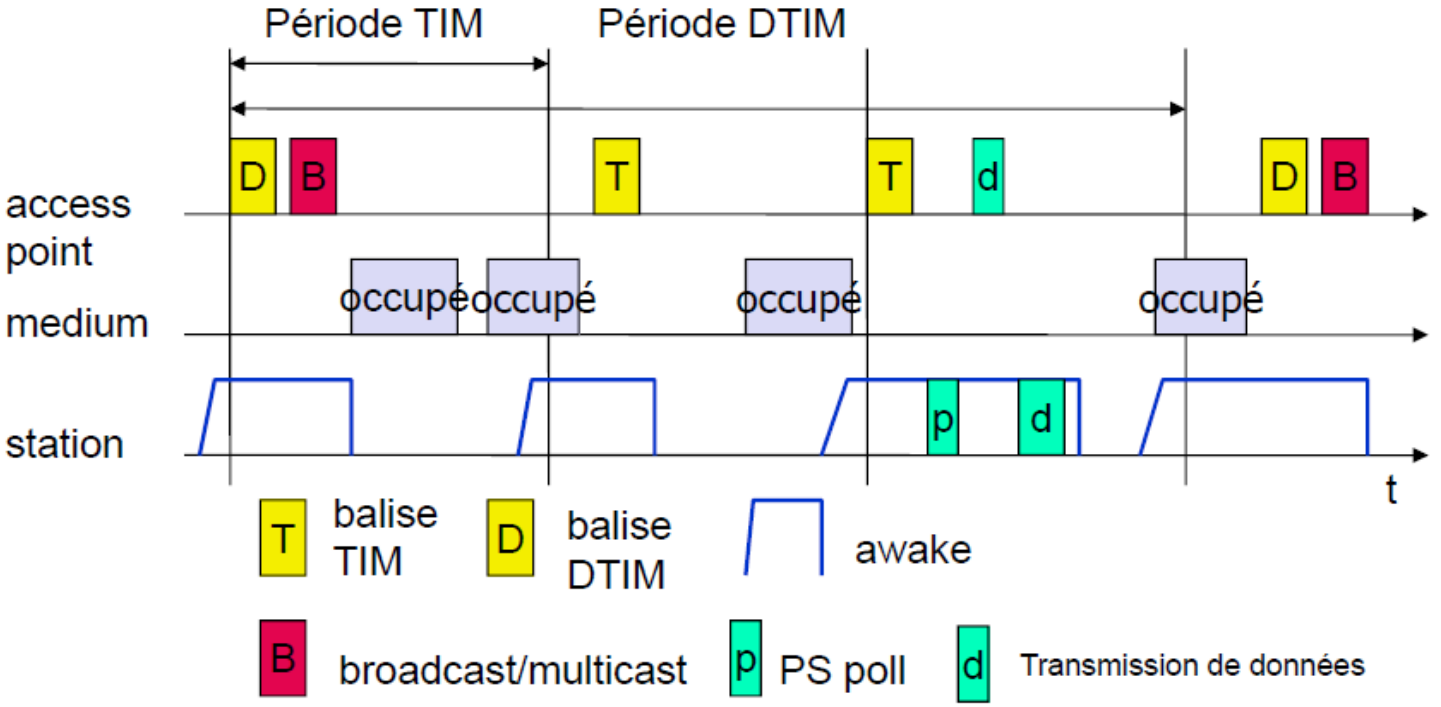
MAC et énergie

- Principe
  - Désactiver le *transceiver* s'il n'est pas utilisé => station peut être dans l'état *sleep/awake*

- La station émettrice
  - a connaissance des stations à économie d'énergie
  - mémorise les paquets des stations dans l'état *sleep*

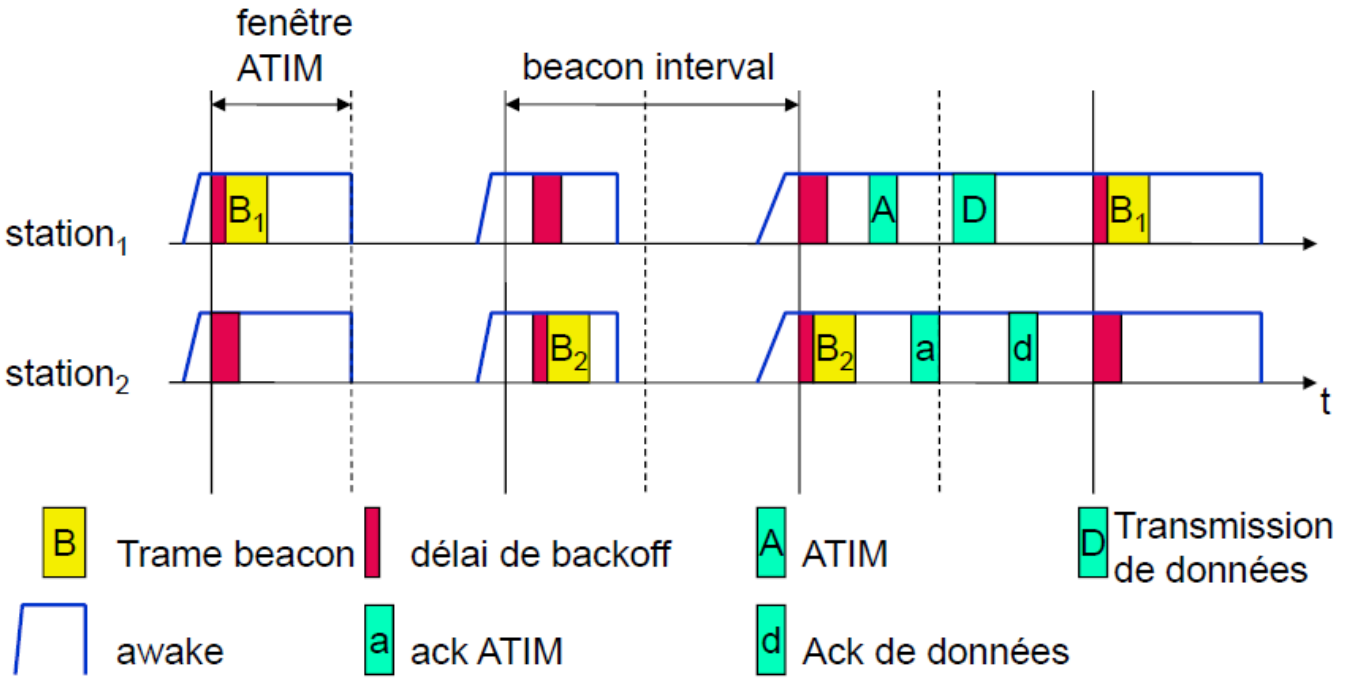
- Grâce à la fonction de synchronisation, les stations passent dans l'état *awake* simultanément
  - en mode infrastructure, pour récupérer
    - *Traffic Indication Map* (TIM)
      - liste des récepteurs de transmission *unicast*
    - *Delivery Traffic Indication Map* (DTIM)
      - liste des récepteurs de transmission *multicast/broadcast*

MAC et énergie



MAC et énergie

- en mode Ad-hoc
  - *Ad-hoc Traffic Indication Map* (ATIM) de chaque nœud possédant des trames pour des stations avec économie d'énergie
  - Liste des récepteurs de transmission *unicast*
  - Une fenêtre temporelle ATIM est prévue pour permettre à toutes les stations d'annoncer leur ATIM



Extensions à IEEE 802.11

- 802.11a,b,g déjà traités
- 802.11e: Amendement de la couche MAC orienté QoS
- 802.11f: Gestion de la mobilité
  - Définition du protocole IAPP (*Inter-Access Point Protocol*)
- 802.11h: Gestion de spectre pour 802.11a
  - Cette extension a été lancée pour répondre au futur problème de la sur-utilisation de la bande 5 Ghz
  - Principalement, 2 nouvelles fonctions sont implémentées:
    - La sélection dynamique de fréquence (DFS: *Dynamic Frequency Selection*) qui permet à un AP de choisir la bande de fréquence qui offrirait les meilleures performances
    - Le contrôle de puissance (TPC: *Transmit Power Control*) qui permet à l'émetteur de contrôler sa puissance et d'émettre qu'à la puissance minimum nécessaire (minimisant les interférences)
- 802.11i: Mécanismes pour améliorer la sécurité offerte par la couche MAC 802.11
  - TKIP améliore WEP tout en restant compatible avec les systèmes à base de WEP
  - AES offre une méthode de chiffrement plus sécurisée
- 802.11k: Méthodes pour mesurer la qualité du canal
  - Définir des mesures et des formats de trames permettant à une station de mesurer/évaluer la qualité d'un canal radio
- 802.11n: Haut débit 100Mbps et plus
  - Extension au niveau des couches physique et MAC pour offrir 100Mbit/s au niveau du MAC SAP
  - Utilisation d'antennes MIMO (*Multiple Input Multiple Output*), un débit théorique allant jusqu'à 600Mbps
- 802.11p: Communications inter-véhicules et panneaux
- 802.11s : réseaux maillés sans fil