UMKB/Département d'Informatique/M1RTIC

Cours :

La couche liaison de données

Dr. AYAD Soheyb

V 1.6

Composée de 2 sous-couches :

LLC : Logical Link Control (802.2)

- Permet d'établir un lien logique entre la couche MAC et la couche de niveau 3 du modèle OSI.
- Elle permet de fiabiliser le protocole MAC par un contrôle d'erreur et un contrôle de flux (LLC 802.2 commun à tous les protocoles MAC 802.x). Ce qui autorise la compatibilité d'un réseau 802.11 avec n'importe quel autre réseau IEEE 802

MAC : Medium Access Control

- Spécifique à l'IEEE 802.11
- Similaire à la couche MAC de l'IEEE 802.3 du réseau Ethernet (c.-à-d. CSMA Carrier Sense Multiple Access)

Rappel sur le CSMA/CD d'Ethernet

- Avant toute tentative de transmission, une station s'assure que le canal n'est pas déjà utilisé (détection de porteuse)
- Si le canal est libre, après une durée aléatoire, la station envoie son paquet
- Plusieurs stations peuvent envoyé en même temps →Collision
- Les stations arrêtent alors de transmettre et tentent de retransmettre en répétant le même processus après des durées aléatoires.

MAC : Medium Access Control 802.11

MAC : Medium Access Control 802.11

Rôle et Principe :

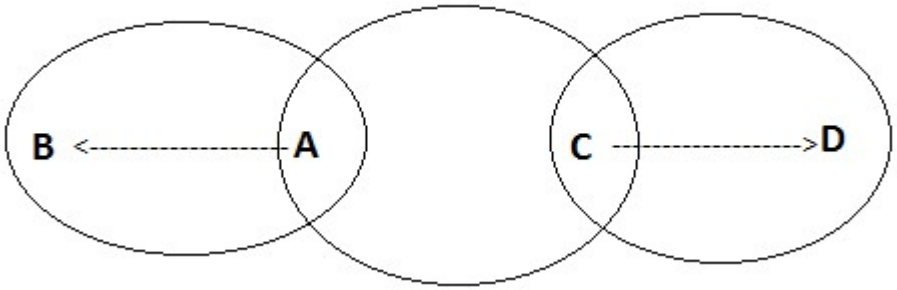
– s’assurer que le support est libre en écoutant la porteuse avant d'émettre

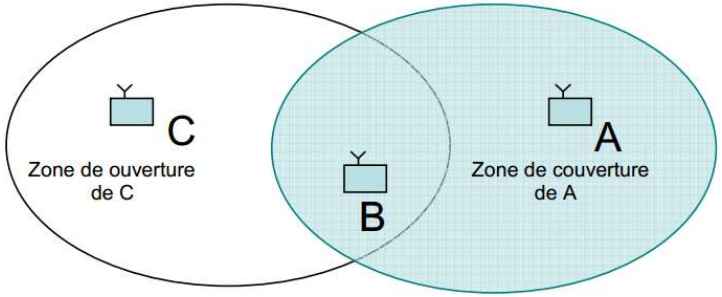
– Si la porteuse est libre, le terminal émet, sinon il se met en attente

Problème de transmission dans les réseaux sans fil

Si les mécanismes de détection de collisions s'avèrent adapté pour un réseau local câblé, ils ne le sont pas, en général, pour les réseaux radio. Plusieurs raisons pour cela :

- on ne peut pas être sûr que toutes les stations s'entendent entre elles (ce qui est l'hypothèse de base du principe de détection de collision), et le fait que la station voulant transmettre teste si le support est libre, ne veut pas forcement dire que le support est libre autour du récepteur.
- Le problème des stations cachées et stations exposées





Particularité du standard

Il définit deux services:

1) Un service qui utilise deux méthodes :
   * La méthode de base repose sur CSMA/CA
   * Cette même méthode peut être augmentée de mécanismes permettant la détection du terminal caché et exposé
2) Un service optionnel qui utilise une méthode sans contention

Une méthode à contention, les ordinateurs qui veulent émettre doivent rivaliser entre eux pour accéder au support. Les rivaux sont départagés par la durée aléatoire du délai d'attente en cas de collision.

- ✓ Les deux premières méthodes connues sous **DCF** Distributed Coordination Function et la 3ième est appelée Point Coordination Function (**PCF**).
- ✓ Les mécanismes MAC sont également appelés Distributed Foundation Wireless MAC (**DFWMAC**)

DFWMAC DCF : Distributed Coordination Function

- Obligatoire
- Possibilité broadcast et multicast
- Tous les utilisateurs qui veulent transmettre ont une chance égale d'accéder au support
- méthode d’accès avec contention

DFWMAC PCF : Point Coordination Function

- Facultative
- Interrogation des terminaux avant transmission (polling)
- Contrôle par le point d'accès
- Conçue pour la transmission de données sensibles
  - *Gestion du délai
  - *Applications de type temps réel : voix, vidéo
- méthode d’accès sans contention

Utilisations :

- Mode ad-hoc uniquement DCF
- Mode infrastructure à la fois DCF et PCF

DCF

DCF

- Repose sur le protocole **CSMA/CA**

(Carrier Sense Multiple Access with Collision Avoidance)

- **Principe :**

1. utilisation d'acquittements positifs (ACK)
2. temporisateurs IFS (Inter-Frame Spacing)
3. écoute du support (NAV)
4. algorithme de Backoff

CSMA/CA

Utilisation d’acquittements positifs (ACK)

CSMA/CA

Évite les pertes de données en utilisant des trames d'acquittement

– ACK envoyé par la station destination pour confirmer que les données sont reçues de manière intacte

CSMA/CA

Temporisateurs IFS
(Inter-Frame Spacing)

CSMA/CA

Accès au support contrôlé par l'utilisation d'espace inter-trame ou IFS (Inter-Frame Spacing)

- Intervalle de temps entre la transmission de 2 trames
- Intervalles IFS = périodes d'inactivité sur le support de transmission
- Il existe différents types d'IFS

CSMA/CA

Temporisateurs IFS

– Permettent d'instaurer un système de priorités
– Pas de garanties fortes

*** SIFS (Short Inter Frame Spacing)**

– La plus haute priorité, ACK, CTS, Réponses aux pollings

*** DIFS (DCF, Distributed Coordination Function IFS)**

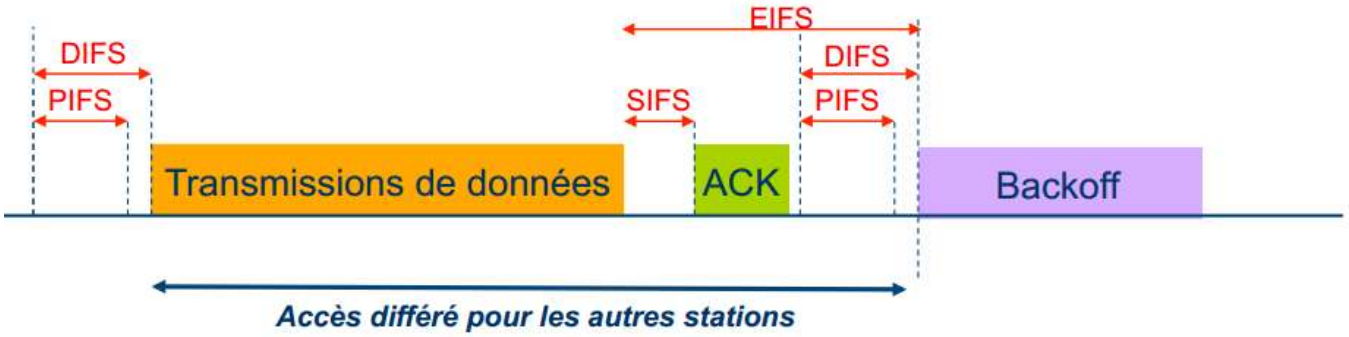
– La plus basse priorité, services de données asynchrones

*** PIFS (PCF IFS)**

– Il permet aux transmissions PCF de gagner l'accès au médium par l'utilisation d'un IFS plus petit que celui utilisé pour la transmission des trames en DCF.

*** EIFS**

– Le plus long, il est utilisé lorsqu'il y a détection de collision. Ce temps relativement long par rapport aux autres IFS est utilisé comme inhibiteur pour éviter des collisions en série ,



CSMA/CA

Calcule des temporisateurs:

Les valeurs des différents **PIFS** et **DIFS** sont calculées de la manière suivante :

PIFS = SIFS + *Slot Time*
DIFS = SIFS + 2 * *Slot Time*

Standard	Durée d'un slot (µs)	DIFS (µs)
IEEE 802.11-1997 (FHSS)	50	128
IEEE 802.11-1997 (DSSS)	20	50
IEEE 802.11b	20	50
IEEE 802.11a	9	34
IEEE 802.11g	9 or 20	28 or 50
IEEE 802.11n (2.4 GHz)	9 or 20	28 or 50
IEEE 802.11n (5 GHz)	9	34
IEEE 802.11ac (5 GHz)	9	34

Norme	SIFS (µs)[1]
IEEE 802.11-1997 (FHSS)	28
IEEE 802.11-1997 (DSSS)	10
IEEE 802.11b	10
IEEE 802.11a	16
IEEE 802.11g	10
IEEE 802.11n (2.4 GHz)	10
IEEE 802.11n (5 GHz)	16
IEEE 802.11ac	16

CSMA/CA

Écoute de support (NAV)

CSMA/CA

– Les terminaux d'un même BSS peuvent écouter l'activité de toutes les stations se trouvant dans le même BSS

– Afin de limiter les risques de collisions, lorsqu'une station envoie une trame

* les autres stations mettent à jour un temporisateur appelée NAV (Network Allocation Vector)
* Le NAV permet de retarder toutes les transmission prévues
* NAV est calculé par rapport à l'information située dans le champ durée de vie dans les trames envoyées

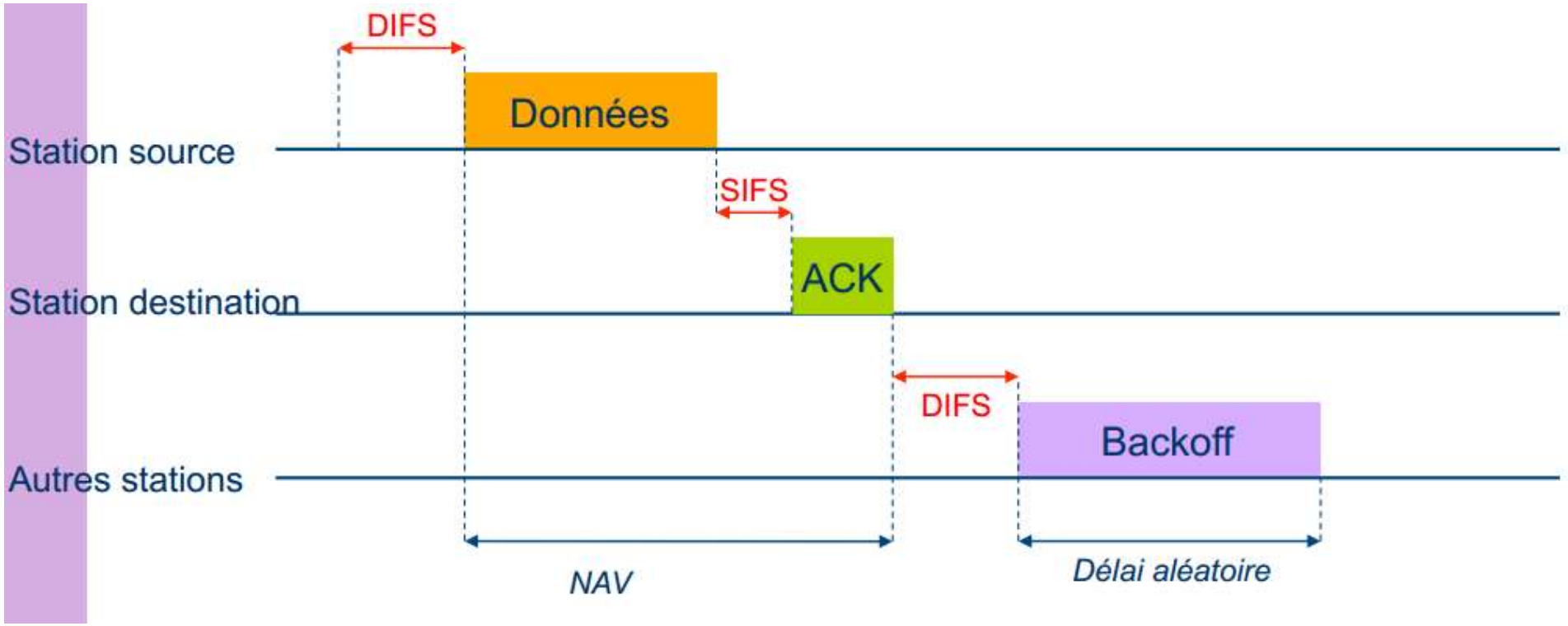
CSMA/CA

- **La station voulant émettre écoute le support**
  - Si aucune activité n'est détectée pendant un DIFS, transmission immédiate des données
  - Si le support est occupé, la station écoute jusqu'à ce qu'il soit libre
    * Quand le support est disponible, la station retarde sa transmission en utilisant l'algorithme de retrait (backoff) avant de transmettre

- **Si les données ont été reçues de manière intacte (vérification du CRC de la trame), la station destination attend pendant un SIFS et émet un ACK**
  - Si l'ACK n'est pas détecté par la source ou si les données ne sont pas reçues correctement, on suppose qu'une collision s'est produite et la trame est retransmise

CSMA/CA

- Exemple de transmission



CSMA/CA

Afin de surveiller l'activité du réseau, la sous couche MAC travaille en collaboration avec la couche physique qui utilise l'algorithme **CCA (Clear Channel Assessment)** pour évaluer la disponibilité du canal.

- Pour savoir si le canal est libre, la couche physique mesure la puissance reçue par l'antenne appelée **RSSI (Received Signal Strength Indicator**).
- La couche physique détermine donc si le canal est libre en comparant la valeur du RSSI à un certain seuil et transmet par la suite à la couche MAC un indicateur de canal libre. Dans le cas contraire, la transmission est différée.

CSMA/CA

Algorithme de retrait (backoff)

CSMA/CA

Le standard 802.11 définit l'algorithme de **backoff** comme devant être exécuté dans les cas suivants :

- Quand la station écoute le support avant la première transmission d'un paquet et que le support est occupé,
- Après chaque retransmission

Le seul cas où ce mécanisme n'est pas utilisé est quand la station décide de transmettre un nouveau paquet et que le support a été libre pour un temps supérieur au DIFS.

Inconvénient :

- Pas de garantie de délai minimal
- Complique la prise en charge d'applications temps réel telles que la voix ou la vidéo

CSMA/CA (backoff)

But : Résoudre les différents entre plusieurs stations voulant avoir accès au support au même temps.

Principe :

- Cette méthode demande a chaque station de choisir un délai d'attente aléatoire **DAA** qui est égale à un certain nombre de TimeSlots,
- Ensuite attendre ce nombre de slots avant de transmettre, toujours en vérifiant qu'une autre station n'a pas accédé au support avant elle.

CSMA/CA

Calcule de DAA

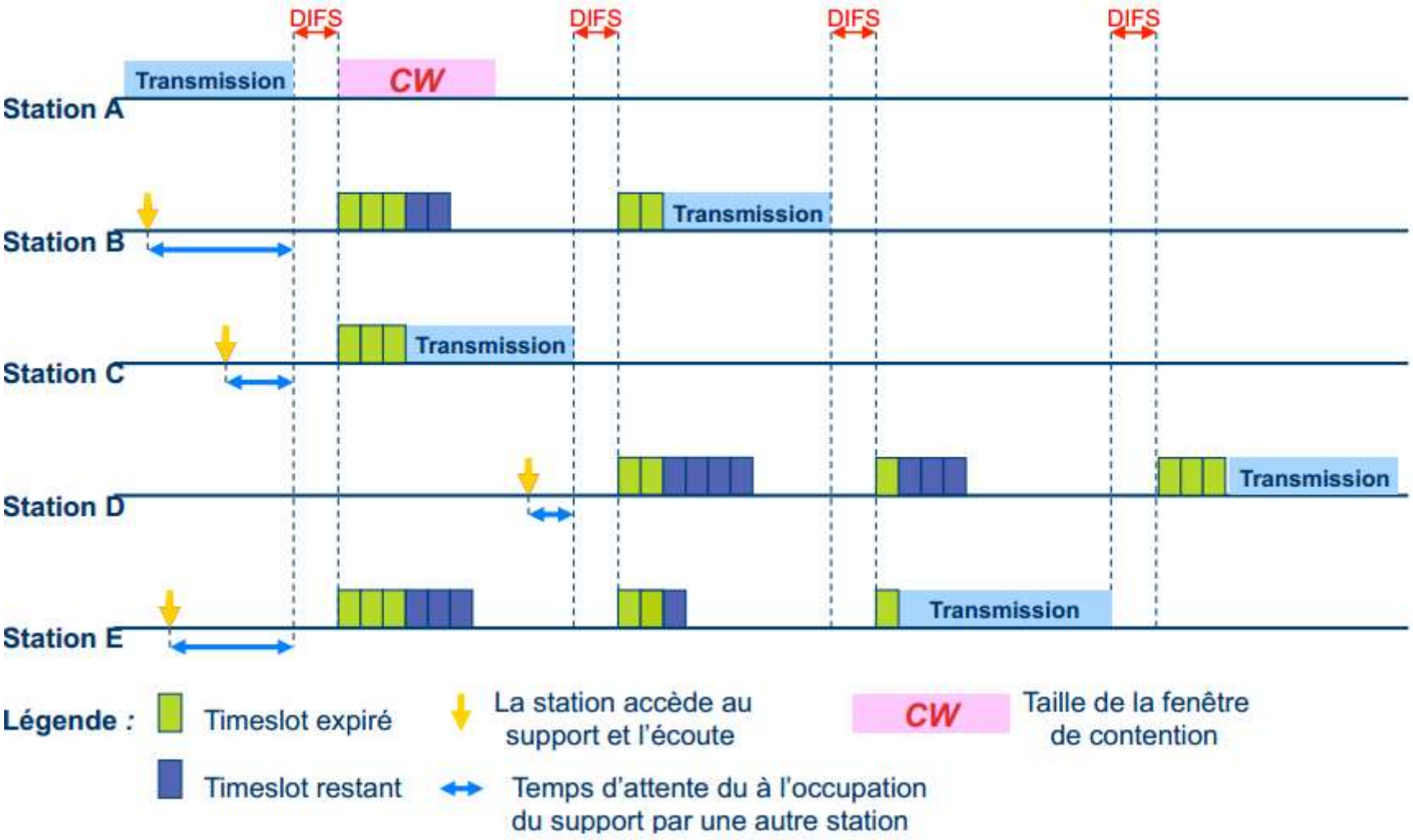
DAA= random(0,CW) * SlotTime

- **random(0,CW)** est une variable aléatoire uniforme comprise entre 0 et CW
- **CW** est la taille de la fenêtre de contention, CW = [CWmin CWmax]
  Lors de la première tentative de transmission, CW = CWmin;
- et à la fois suivante (en cas de collision) CW est doublée jusqu'à ce qu'elle atteigne **CWmax**.

Exemple wifi :

CWmin= 31
CWmax=1023

CSMA/CA


DIFS
DIFS
DIFS
DIFS
Transmission
CW
Station A
Station B
Transmission
Station C
Transmission
Station D
Transmission
Station E
Transmission
Légende :
Timeslot expiré
Timeslot restant
La station accède au support et l'écoute
Temps d'attente du à l'occupation du support par une autre station
CW
Taille de la fenêtre de contention

CSMA/CA

- **Que se passe-t-il en cas de mauvaise réception ?**

- **EIFS est défini comme tel dans le standard**
  – «L'**EIFS** doit être utilisé par le mode DCF à chaque fois que la couche PHY indique à la couche MAC qu'une transmission a commencé et qu'elle ne résulte pas en une réception correcte de la trame MAC avec une valeur FCS correcte »

Mécanisme CSMA/CA avec échange de messages courts RTS et CTS

DFWMAC DCF avec réservation

Principe

- Envoi de trames RTS/CTS (Request To Send/Clear To Send) entre une station source et une station destination avant tout envoi de données.
- Station qui veut émettre envoie un RTS: Toutes les stations du BSS entendent le RTS, lisent le champ de durée du RTS et mettent à jour leur NAV
- Station destination répond après un SIFS, en envoyant un CTS: Les autres stations lisent le champ de durée du CTS et mettent de nouveau à jour leur NAV.
- Après réception du CTS par la source, celle-ci est assurée que le support est stable et réservé pour la transmission de données .

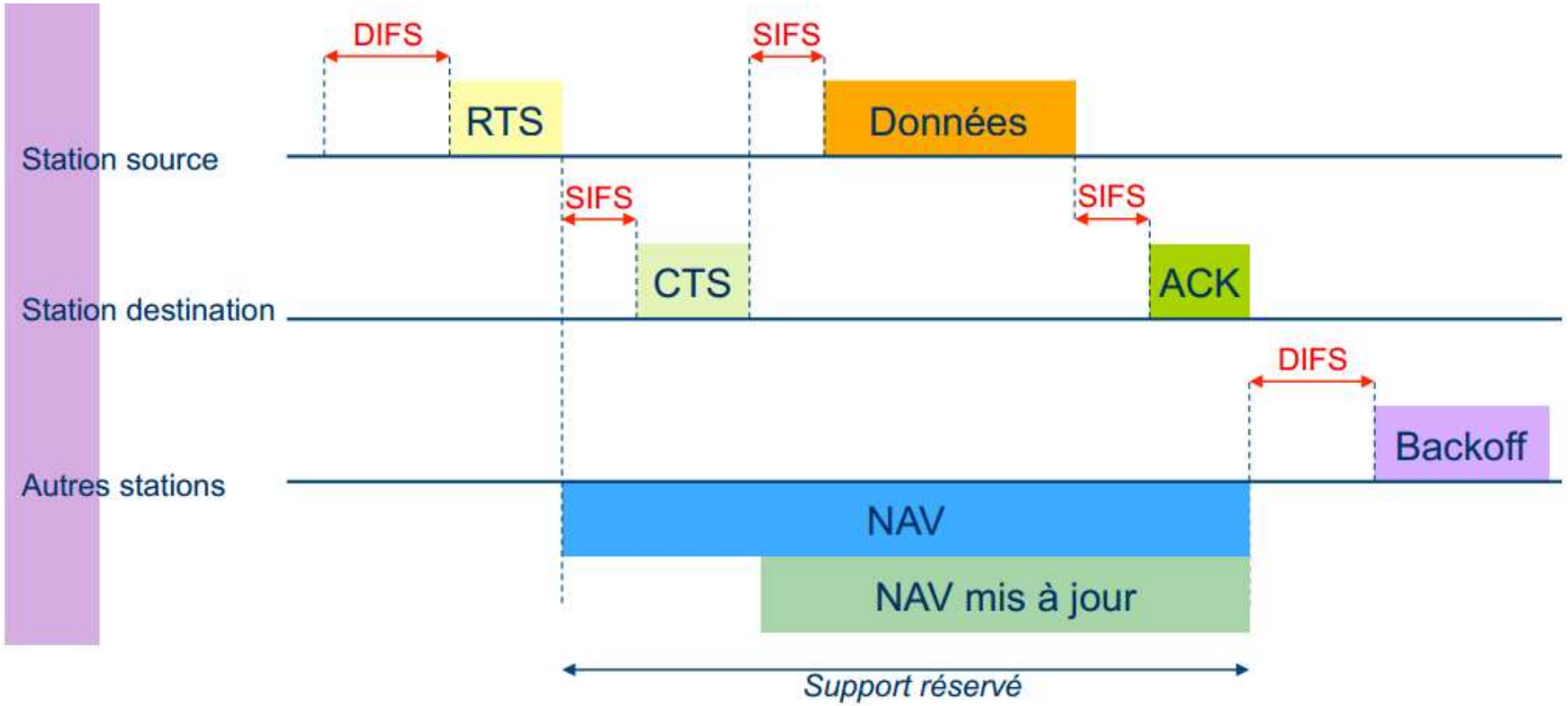
DFWMAC DCF avec réservation

Caracteristiques

- Assure une transmission des données et réception de l'ACK sans collision
- Trames RTS / CTS réservent le support pour la transmission d'une station
  - Mécanisme habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante
- Les stations peuvent choisir d'utiliser le mécanisme RTS / CTS ou pas

DFWMAC DCF avec réservation

Transmission avec mécanisme de réservation



DFWMAC DCF avec réservation

Le mécanisme de RTS / CTS permet de résoudre aussi les problèmes suivants:

- Problème de la station cachée

2 stations situées chacune à l'opposé d'un point d'accès (AP) ou d'une autre station

- peuvent entendre l'activité de cet AP
- ne peuvent pas s'entendre l'une l'autre du fait que la distance entre les 2 est trop grande ou qu'un obstacle les empêche de communiquer entre elles

- Problème des stations exposées

DFWMAC DCF avec réservation

➢ **Inconvénient** :

Ajout d'en-têtes aux trames 802.11

– Performances plus faibles que les réseaux locaux Ethernet

Fragmentation – réassemblage

DFWMAC DCF avec réservation

Fragmentation – réassemblage

– La fragmentation accroît la fiabilité de la transmission en permettant à des trames de taille importante d'être divisées en petits fragments

- Réduit le besoin de retransmettre des données
- Augmente les performances globales du réseau

– Fragmentation utilisée dans les liaisons radio, dans lesquelles le taux d'erreur est important

- + la taille de la trame est grande et + elle a de chances d'être corrompue
- Lorsqu'une trame est corrompue, + sa taille est petite, + la durée nécessaire à sa retransmission est faible

DFWMAC DCF avec réservation

Fragmentation – réassemblage

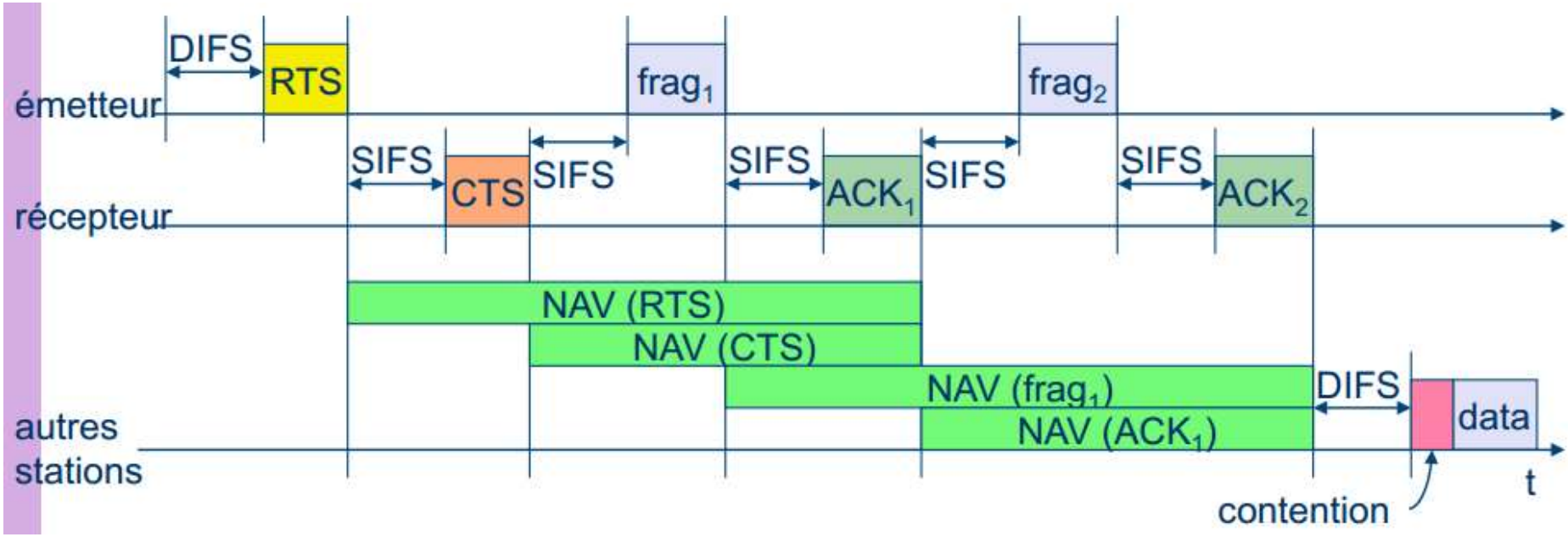
– Pour savoir si une trame doit être fragmentée, on compare sa taille à une valeur seuil

– Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle

- Le support n'est libéré qu'une fois tous les fragments transmis avec succès
- Si un ACK n'est pas correctement reçu, la station arrête de transmettre et essaie d'accéder de nouveau au support et commence à transmettre à partir du dernier fragment non acquitté
- Si les stations utilisent le mécanisme RTS/CTS, seul le premier fragment envoyé utilise les trames RTS / CTS

DFWMAC DCF avec réservation

- **Schéma avec fragmentation**



Trames MAC 802.11

Trames MAC 802.11

- Il y a trois principaux types de trames :

  - Les trames de **données**, utilisées pour la transmission des données

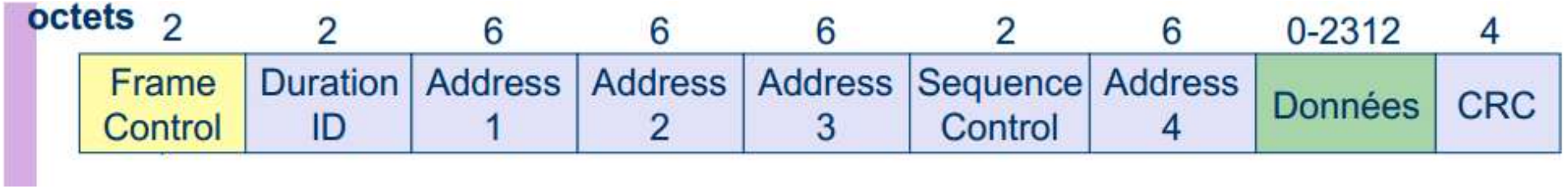
  - Les trames de **contrôle**, utilisées pour contrôler l'accès au support (eg. RTS, CTS, ACK)

  - Les trames de **gestion**, sont envoyés de la même façon que les trames de données (c-à-d : réservation des liens avec les trames de contrôles !) pour la gestion des connexions

- Chacun de ces trois types est subdivisé en différents sous-types, selon leurs fonctions spécifiques.

Format des trames MAC

802.11 – format de trame MAC



Format des trames MAC

Frame control (2 octets)

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt.	More Data	Protected Frame	+HTC/ Order

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt.	More Data	Protected Frame	+HTC/ Order

- **Version** : 2 bits permettant de connaître la version 802.11
- **Type/sous-type** : 6 bits qui définissent le type de trames :
  - 00 Gestion : échange d'info de gestion tel que requête/réponse de (ré)association, Balise, ATIM, Authentification….
  - 01 Contrôle : pour le contrôle d'accès au support (RTS, CTS, ACK,PS
  - 10 données : transfert des données avec ou sans ACK

Gestion

type	sous-type	Description du sous type
00	0000	Requête d'association
00	0001	Réponse d'association
00	0010	Requête de ré-association
00	0011	Réponse de ré-association
00	0100	Demande de sonde
00	0101	Réponse de sonde
00	0110-0111	Réservés
00	100	Balise (BEACON)

Contrôle

01	0000-1001	Réservés
01	1010	PS-Poll
01	1011	RTS
01	1100	CTS
01	1101	ACK
01	1110	CF End
01	1111	CF End et CF-ACK

Données

10	0000	Données
10	0001	Données et CF-ACK
10	0010	Données et CF-Poll
10	0011	Données, CF-ACK et CF-Poll
10	0100	Fonction nulle (sans données)
10	0101	CF-ACK (sans données)
10	0110	CF-Poll (dans données)
10	0111	CF-ACK et CF-Poll (sans données)
10	1000-1111	Réservés

Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt.	More Data	Protected Frame	+HTC/ Order

- ToDS (pour le système de distribution) : ce bit est mis à 1 lorsque la trame est adressée au Point d'Accès pour qu'il l'a fasse suivre au DS (Distribution System).

- FromDS (venant du système de distribution) : ce bit est mis à 1 quand la trame vient du DS.

- More Fragments (d'autres fragments) : ce bit est mis à 1 quand il y a d'autres fragments qui suivent le fragment en cours.

- Retry (retransmission) : ce bit indique que le fragment est une retransmission d'un fragment précédemment transmis. Ceci sera utilisé par la station réceptrice pour reconnaître des transmissions doublées de trames, ce qui peut arriver si un paquet d'accusé de réception se perd.

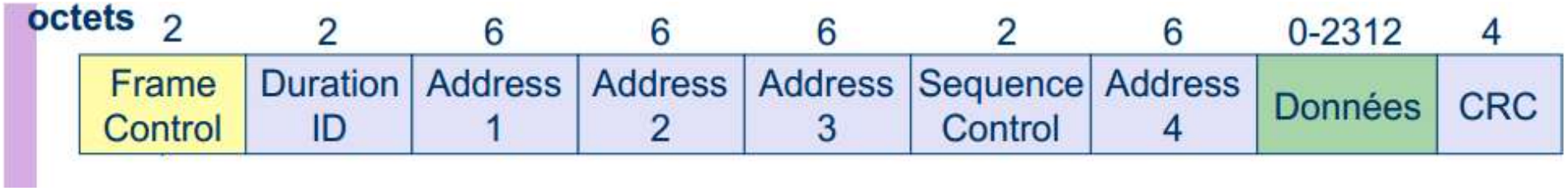
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt.	More Data	Protected Frame	+HTC/ Order

- **Power Management (gestion d'énergie) :** ce bit indique que la station sera en mode de gestion d'énergie après la transmission de cette trame. Ceci est utilisé par les stations changeant d'état, passant du mode d'économie d'énergie au mode active ou le contraire.

- More Data (d'autres données) : ce bit est également utilisé pour la gestion de l'énergie. Il est utilisé par le Point d'Accès pour indiquer que d'autres trames sont stockées pour cette station. La station peut alors décider d'utiliser cette information pour demander les autres trames ou pour passer en mode actif.

- **Protected frame :** indique le WLAN est crypté

- **Order** : ce bit indique que cette trame est envoyée en utilisant la classe de service strictement ordonné (Strictly-Ordered service class). Cette classe est définit pour les stations qui ne peuvent pas accepter de changement d'ordre entre les trames.



Duration ID

Ce champ à deux sens, dépendant du type de trame :

- Pour les trames de polling, c'est l'ID de la station
- Dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV.

Les champs adresses (en-tête MAC)

Une trame peu contenir jusqu'à 4 adresses, selon le bit **ToDS** et **FromDS** définit dans le champ de contrôle, comme suit :

Adresse 1 est toujours l'adresse du récepteur. Si ToDS est à 1, c'est l'adresse du Point d'Accès

Adresse 2 est toujours l'adresse de l'émetteur. Si FromDS est à 1, c'est l'adresse du Point d'Accès

Adresse 3 est l'adresse de l'émetteur original quand le champ FromDS est à 1. Sinon, et si ToDS est à 1, Adresse 3 est l'adresse destination.

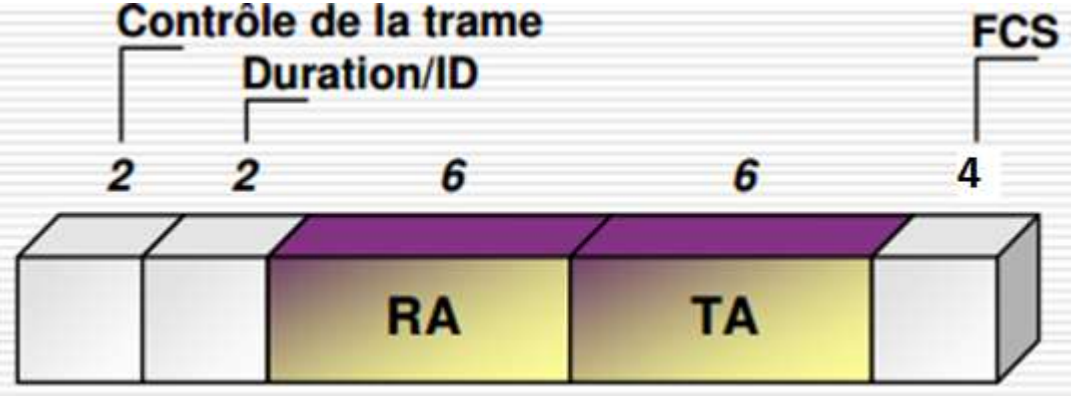
Adresse 4 est utilisé dans un cas spécial, quand le système de distribution sans fil (Wireless Distribution System) est utilisé et qu'une trame est transmise d'un Point d'Accès à un autre. Dans ce cas, ToDS et FromDS sont tous les deux à 1 et il faut donc renseigner à la fois l'émetteur original et le destinataire.

vers DS	De DS	Adresse 1	Adresse 2	Adresse 3	Adresse 4
0	0	DA	SA	BSSID	-
0	1	DA	BSSID	SA	-
1	0	BSSID	SA	DA	-
1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

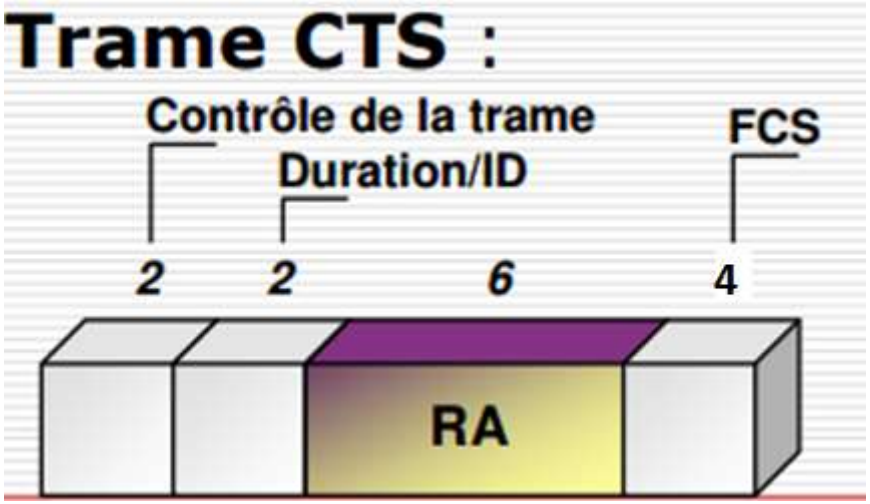
Trame d'une station vers une autre dans le même BSS
Trame venant du système de distribution (DS)
Trame destinée au système de distribution (DS)
Trame envoyée entre les Points d'accèes

Format des trames RTS



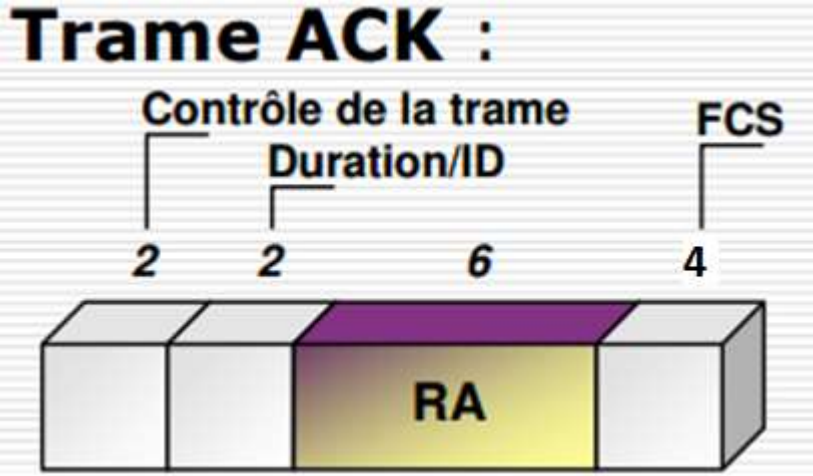
- RA est l'adresse du récepteur
- TA est l'adresse de la station qui transmet la trame RTS.
- La valeur de la durée est le temps, en microsecondes, nécessaire à la transmission de la trame de gestion ou la données suivantes, plus une trame CTS, plus une trame ACK, plus 3 intervalles SIFS.

Format de la trame CTS



- RA est l'adresse du récepteur de la trame CTS, directement copiée du champ TA de la trame RTS.
- La valeur de la durée est la valeur obtenue dans la trame RTS, moins le temps de transmission, en microsecondes, de la trame CTS et d'un intervalle SIFS.

Format de la trame ACK



- RA est le champ directement copié du champ **Adresse 2** (émetteur) de la trame précédent cette trame ACK.
- Si le bit **More Fragment** était à **0** dans le champ de contrôle de trame de la trame précédente, la valeur de la durée est mise à 0. Sinon, c'est la valeur du champ durée précédent, moins le temps, en microsecondes, demandé pour transmettre la trame ACK et l'intervalle SIFS.

Trames de Gestion

Trames de gestion

Les trames de gestion 802.11 permettent à des stations d'établir et de maintenir des communications. - Les principales trames de gestion 802.11 sont les suivantes :

- **Trame de "Beacon" (écoute passif du client)**
  - Un point d'accès envoie périodiquement des trames "BEACON FRAME" pour annoncer sa présence et relayer des informations, tel le SSID et d'autres paramètres.
  - Les mobiles écoutent "continuellement" tous les canaux et donc entendent les trames BEACON qui sont à la base du choix du canal.
- **Trame de demande de sonde (Probe request) (écoute active du client)**
  - Une station envoie une trame de demande de sonde quand elle a besoin d'obtenir des informations d'une autre station.
  - Par exemple : un mobile envoie une demande de sonde pour déterminer quels sont les points d'accès à sa portée.
- **Trame de réponse de sonde**
  - Une station répond avec une trame de réponse de sonde, contenant des informations de capacités, débits supportés, etc., après avoir reçu une trame de demande de sonde.

Trames de gestion

- **Trame d'authentification :** processus par lequel le point d'accès accepte ou rejette l'identité d'un mobile.
  - système ouvert (par défaut) :
    - le mobile envoie une trame d'authentification
    - L'AP répond avec une trame d'authentification indiquant l'acceptation.
  - facultative clé partagée : envoi de 4 trames d'authentification
    - le mobile envoie une première trame,
    - L'AP répond en joignant son texte de défi
    - Le mobile renvoie une version chiffrée du texte de défi
    - Le point d'accès informe le mobile du résultat de l'authentification.

- **Trame de désauthentification**
  - Une station envoie une trame de désauthentification à une autre station si elle souhaite terminer ses communications.

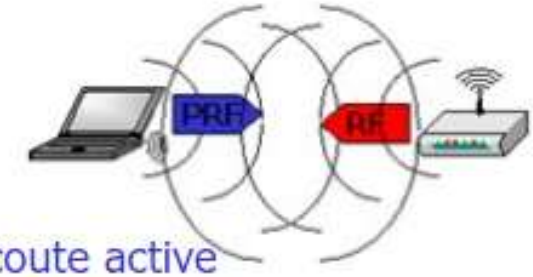
Trames de gestion

- **Trames d'association**
  - Permet à l'AP d'allouer des ressources pour un mobile et de les synchroniser avec lui.
    - Un mobile envoie une demande d'association à un AP, qui contient les informations du mobile (par exemple, débits supportés) et le SSID du réseau avec qui il souhaite s'associer.
    - L'AP considère s'associer au mobile et (si admis) réserve l'espace mémoire et établit une identification d'association pour le mobile et répond en notifiant le mobile d'informations telles que l'identification d'association et les débits supportés.
- **Trames de réassociation (requête et réponse)**
  - Servent lorsqu'un mobile trouve un autre AP ayant un signal plus fort, le mobile enverra une trame de réassociation au nouveau point d'accès.
- **Trame de désassociation**
  - Sert à une station à informer une autre station qu'elle souhaite terminer l'association. Le point d'accès peut alors abandonner les allocations de mémoire et enlever le mobile de la table d'association.

Processus de connexion dans un BSS

- Après allumage, mode veille ou déplacement géographique, une station veut joindre un BSS
- Synchronisation sur l'AP (ou sur les autres stations dans le mode ad hoc)
  - Par écoute passive : écoute des trames balise (*beacon*) émises périodiquement par l'AP
  - Ou par écoute active : émission d'une requête *Probe Request Frame*, et attente de la réponse de l'AP
- Authentification : L'AP et la station se prouvent leur identité (par connaissance d'un mot de passe). Un « mode ouvert », sans authentification existe aussi.
- Association : échange d'information sur les stations de la cellule et leur capacité, enregistrement de la position des stations par l'AP

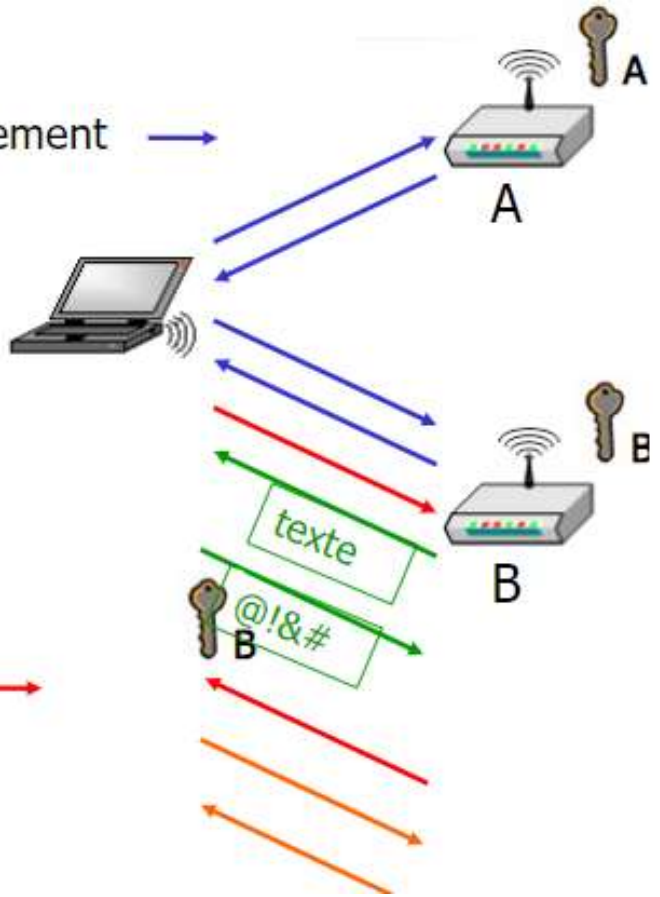
Ecoute passive



WLAN Ecoute active

Authentification et association

- La station diffuse une demande d'enregistrement →
- Les points d'accès répondent →
  - La station évalue la réponse et sélectionne le meilleur point d'accès
- La station émet une trame « demande d'authentification » →
- Le PA envoie un texte →
- La station chiffre le texte avec la clé d'authentification de l'AP →
- Le PA confirme l'authentification du poste →
- La station envoie une demande d'association à l'AP →
- L'AP confirme l'association →



Débit théorique et débit utile dans 802.11

- Les débits de 802.11b sont compris entre 1 et 11 Mbit/s.

- Les débits annoncés ne sont que des valeurs théoriques, par exemple le débit 11 Mbit/s de la norme 802.11b correspond approximativement à 5 Mbit/s de débit utile. De même pour 802.11a et 802.11g.

- Cette différence s'explique essentiellement par la taille des en-têtes des trames utilisées dans 802.11. Ainsi que par l'utilisation d'un certain nombre de mécanismes qui permettent de fiabiliser la transmission dans un environnement radio.

- Les débits annoncés par les différents standards, 802.11b, 802.11a et 802.11g, correspondent à la vitesse de transmission sur l'interface sans fil et non à des débits réels.

- Comme nous l'avons vu précédemment, les données envoyées sur cette interface correspondent à une trame physique, ou PLCP-PDU.

- L'en-tête PCLP-PDU comporte deux champs, le préambule PLCP et l'en-tête PLCP.

- Deux types de préambules sont définis, un long et un court. Un préambule long permet de fiabiliser la connexion au réseau et donc les transmissions.

- Chaque partie de la PLCP-PDU est envoyée à des vitesses différentes.

- L'en-tête PLCP-PDU est transmis à 1 Mbit/s dans le cas du préambule long. Pour un préambule court, le préambule PLCP est transmis à 1 Mbit/s et l'en-tête PLCP à 2 Mbit/s.

- Le troisième champ de la PLCP-PDU correspond à la trame MAC elle-même. Cette dernière est envoyée à des débits pouvant aller de 1 – 2 - 5,5 ou 11 Mbit/s pour ce qui concerne 802.11b.

Calcule du débit utile

- Afin de calculer le **débit utile *Du*** de transmission d'une **donnée**, il faut connaître le **temps de transfert *T*** équivalent.

- ***T***est lié au **temps de transmission** augmenté **temps de propagation.**

$$T_{transfert} = T_{transmission} + T_{propagation}$$

$$T_t = (T_{(en-tête\ PLCP-PDU)} + T(_{MPDU}) + T_{(Propagation)}$$

Remarque : dans un milieu ouvert et sans obstacle le temps de propagation est considéré nul étant donné qu'il est équivalent à la vitesse de la lumière.

Fin.