Réseaux sans fil
IEEE 802.11

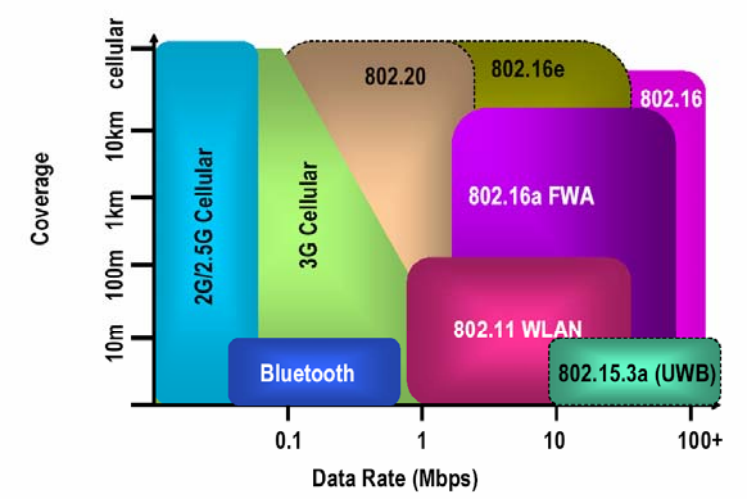
Bernard Cousin

Un réseau local sans fil

- C'est quoi ?
  - Un ensemble de stations fixes ou mobiles, interconnectées par un réseau local de communication radio
- Ca sert à quoi
  - Offrir un moyen de communications numériques entre ces stations
  - Facile à déployer (… sans fil !)
- 1990 : lancement du groupe de travail à l'IEEE
  - 1997 : IEEE 802.11 - "Wireless Local Area Network" (WLAN)

    "IEEE Standard for Information Technology-
    Telecommunications and Information Exchange Between Systems-
    Local and Metropolitan Area Networks- Specific Requirements-
    Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"

Les réseaux sans fil



Caractéristiques de l'IEEE 802.11

- Communications
  - Directes :
    - d'une station (fixe ou mobile) à une autre station (fixe ou mobile)
    - sans relayage
  - Indirectes :
    - En passant par une (ou des) station(s)
      - Station de base
      - Ou avec routage (réseau ad'hoc)
- Utilisation de bandes de fréquence
  - 2,4 Ghz (ISM : "Industrial, Scientific and Medical"), 5 GHz (U-NII : Unlicenced-National Information Infrastructure), ou Infrarouge
  - Sans licence d'exploitation
  - Libres dans de nombreux pays
- Débits variables
  - Adaptation aux conditions de l'environnement radio
  - Différents codages (FHSS, DSSS, OFDM, etc.)

Caractéristiques de l'IEEE 802.11

- Portée locale
  - Typiquement : 30 m en intérieur, 100 m en extérieur
- La technique d'accès au support partagé
  - "Medium Access Control"
  - Complexe :
    - S'adapte à une large gamme de fréquences
      - 2,4 GHz, 5 GHz, IR
    - Propose de nombreuses options
      - avec infrastructure ou adhoc, contrôle d'accès distribué ou centralisé, avec ou sans économie d'énergie, etc.
  - CSMA/CA
    - "Carrier Sense Multiple Access/Collision Avoidance"
    - Similaire mais différent du CSMA/CD d'Ethernet :
      - La détection de collision est impossible

Plan

- Présentation des réseaux locaux sans fil
- Architecture des réseaux locaux sans fil
- Couche Physique
- Couche Liaison de Données

Bibliographie

- William Stallings. Réseaux et communicartion sans fil. Pearson Education, 2005.
- Pejman Rosham, Jonathan Leary. Réseaux WiFi : notions fondamentales. Cisco Press. 2004
- Matthew S. Gast. 802.11 Wireless Networks. O'Reilly. 2005.

- Certains transparents ou figures sont issus de :
  - Yassine Hadjadj (université de Rennes 1)

Les normes 802.11

- IEEE 802.11 – Les réseaux locaux sans fil
  - 802.11 : 1-2 Mbit/s (IR, FHSS, DSSS)
  - 802.11a : 6-54 Mbit/s (OFDM, bande 5 GHz, et avec licence bande 3,7 GHz)
  - 802.11b : 5,5-11 Mbit/s (DSSS, bande ISM 2,4 GHz)
  - 802.11g : <54 Mbit/s (DSSS, bande ISM 2,4 GHz)
  - 802.11n (MIMO) : <150 Mbit/s (bande ISM 2,4 GHz/5 GHz)
  - 802.11ad : Très haut débit "wiHD" (60 GHz), regroupé avec 802.15.3c

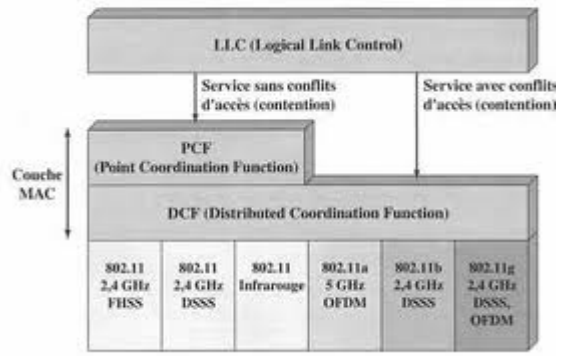
  -.-.-
  - 802.11c : Pontage
  - 802.11e : Qualité de service
  - 802.11i : Amélioration de la sécurité WEP=>WAP2
  - 802.11f : "Inter-Access Point Protocol" - Itinérance ("Roaming" => "Hand-over")
  - 802.11r : "fast BSS transition"

L'architecture en couches

Couche 2 de l'OSI	Logical Link Control (LLC)						
	Medium Access Control (MAC)						
Couche 1 de l'OSI	PLCP						
	PMD	FHSS	DSSS	IR	"Wi-Fi" 802.11b	"Wi-Fi" 802.11g	"Wi-Fi5" 802.11a

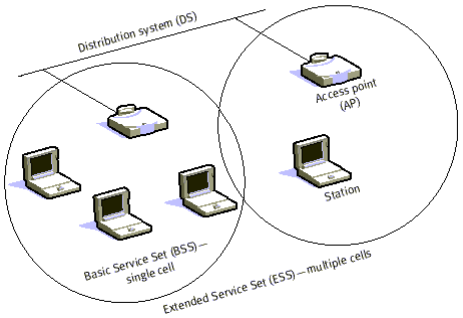
- PLCP Physical Layer Convergence Protocol
- PMD : Physical Medium Dependent

L'architecture en couches



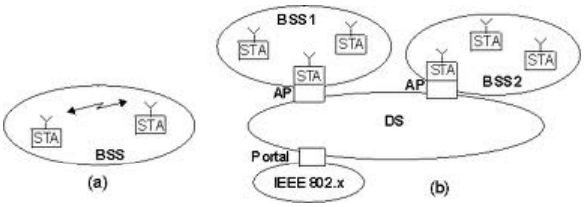
Services et entités d'un réseau 802.1

- Service de communication
  - BSS : Dans une seule cellule ("basic set area")
  - ESS : Ensemble de cellules
- Entre
  - Stations (STA)
  - Point d'accès (AP)
- Interconnectés (ou pas)
  - Par un système de distribution (DS)



Modes de fonctionnement de IEEE 802.11

- Deux modes de fonctionnement
  - Avec infrastructure ("with AP")
  - Sans infrastructure, appelé aussi adhoc



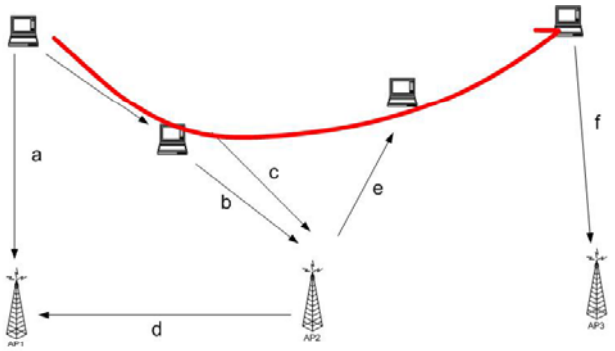
Le mode avec infrastructure

- Les points d'accès (AP) sont responsables :
  - des services spécifiques
    - contrôle d'accès, authentification, gestion de l'association
  - sur leur zone de couverture
  - ils jouent aussi le rôle de station (STA) dans un BSS
  - un BSS est identifié par son BSSID
- Le système de distribution (DS)
  - accroît le champ de communication au-delà de la couverture radio
  - offre aux usagers des STA l'accès à d'autres ressources
    - serveurs de fichiers, imprimantes, et au reste de l'Internet (dont d'autres réseaux mobiles avec d'autres types ou non)

Les services

- Les services des Stations:
  - authentication,
  - de-authentication,
  - privacy,
  - delivery of data
- Les services du Système de Distribution (DS) *(A thin layer between MAC and LLC sublayer)*
  - association
  - disassociation
  - reassociation
  - distribution
  - Integration

Etats lors d'une mobilité



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

Les Services

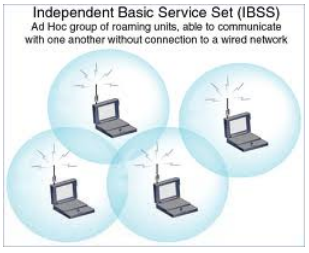
- Authentification
  - **"Open System Authentication":**
    - sans réelle authentification, puisque n'importe quelle station se connectant est admise.
  - **"Shared Key Authentication":**
    - basée sur un partage de clé secrète entre la station et le point d'accès. Si la station utilise une clé différente du PA, il y a rejet. Ce mécanisme peut être activé avec les protocoles de sécurité WEP, WAP, WAP2, etc.
- Dé-authentification
  - Permet l'élimination d'une STA précédemment authentifiée.
- Transfert de données
  - Le transfert fiable et efficace de trames de données

Les Services

- Association
  - Permet la création d'un lien logique entre STA et PA
  - Nécessaire avant tout échange de paquets de données afin de connaître les paramètres de l'échange
- Désassociassion:
  - Permet au PA de forcer la STA à éliminer l'association
    - Exemple: cas d'un manque de ressources dans un PA
  - Permet à la STA d'informer le PA d'un départ
- Réassociation
  - Permet à la STA de se réassocier après une perte du signal du PA courant => "Hand-over"
  - Equivalent à une association à l'exception des trames concernant le dernier PA
  - Nécessaire pour permettre au nouveau PA de demander à l'ancien PA de récupérer les trames en attente d'envoi à la STA
- Distribution
  - Utilisé chaque fois que la STA doit envoyer des trames en passant par le système de distribution
  - Permet d'obtenir des informations sur le bon BSS pour la trame
- Intégration
  - Permet de connecter un WLAN 802.11 à d'autres LAN
  - Conversion des trames 802.11 dans un autre format

Mode ad hoc

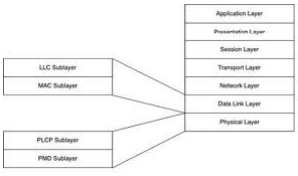
- Un réseau local sans fil fonctionnant en mode ad hoc
  - ne nécessite aucune infrastructure préalablement déployée pour permettre la communication entre ses stations
  - Chaque station opère de manière autonome afin d'assurer sa connectivité et celle des autres membres
  - Au minimum deux stations dans la couverture radio l'une de l'autre
  - Le groupe de stations forment un IBSS ("Independent Basic Service Set")



IEEE 802.11
La couche Physique

La couche Physique de l'IEEE 802.11

- But :
  - Transmission sans fil (radio ou IR) des données entre les stations du réseau local
    - Établissement et maintien de la qualité
  - Test de l'état du canal radio (ou IR) :
    - Occupé ou disponible
- Indépendance des services offerts à la couche MAC
  - "Physical Layer Convergence Protocol" (PLCP)
    - Indépendance vis-à-vis de la technologie
  - "Physical Medium Dependent" (PMD)
    - Une pour chaque technologie



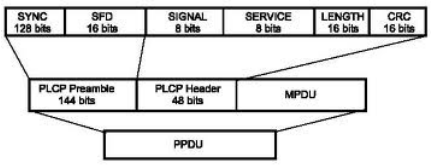
Transmission infrarouge

- Le rayonnement infrarouge (IR)
  - un rayonnement électromagnétique d'une longueur d'onde supérieure à celle de la lumière visible mais inférieure à celle des micro-ondes.
    - 780 nm à 1 mm (0,5 THz à 350 THz).
  - Les objets émettent spontanément des radiations infrarouges :
    - À température ambiante, le maximum d'émission naturelle se situe aux alentours de 10 µm.
  - Les transmission IR
    - Sont directionnelles
      - L'émetteur et le récepteur doivent être en vue directe
      - Ou bien utiliser un mode de transmission diffus !
        - réflexion sur le plafond, par exemple
    - Modulation simple
      - Par amplitude (pas par phase ni fréquence)
      - Modulateurs peu coûteux
    - Les débits sont limités
      - 2 Mbit/s pour l'IEEE 802.11
    - La portée est limitée
      - Environ 10 m
      - Les IR traversent pas les murs
    - Ne nécessitent pas d'allocation des fréquence (sans licence)

Transmission radio

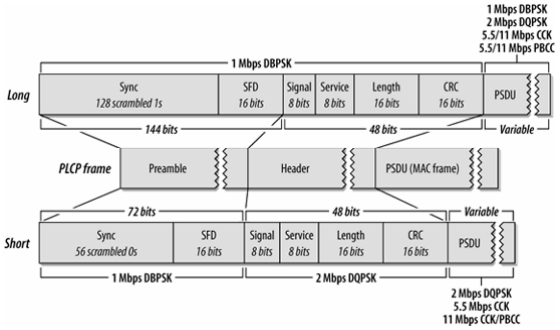
- Plages de fréquences
  - Bande ISM : 2,4 GHz
  - Bande U-NII : 5 GHz
  - Bande 60 GHz
- Transmission omnidirectionnelle
  - Sans utilisation d'antenne parabolique (contrairement aux micro-ondes)
- S'accommode des obstacles opaques
- Souffre
  - Des trajets multiples
    - Provoqués par les matériaux réfléchissants
  - Des atténuations
    - provoquées par les matériaux absorbants
  - Des interférences
    - avec les autres utilisateurs des mêmes fréquences

Format des trames PLCP



- Synchronisation
  - Une suite binaire de "0" et de "1" (12 symboles OFDM pour IEEE 802.11a)
  - Compensation de la fréquence
  - Détection de l'énergie
    - configuration du gain, choix du codage
- "Start Frame Delimiter"
  - "11110011 10100000"
- Signal
  - Débit de la transmission
    - 0x0A : 1 Mbit/s par DBPSK, 0x14 : 2 Mbit/s par DQPSK, 0x 37 : 5,5 Mbit/s, 0x6E : 11 Mbit/s
- Service
  - 00 : compatible 802.11
- "Length"
  - Longueur de champ de données (en ms)
- "Header Error Checksum"
  - CRC : x^16 + x^12 + x^5 + 1 (le CRC -16 d'HDLC !)

Format court des trames PLCP



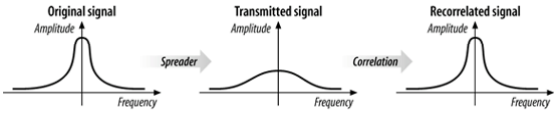
- Propose un format court
  - IEEE 802.11b
  - Réduit l'overhead
    - À 11 Mit/s, le préambule devient prépondérant
  - SDFinverse = 0000 0101 1100 1111

Etalement en fréquences

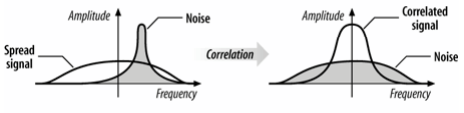
- The radio-based physical layers in 802.11 use three different spread-spectrum techniques:
  - Frequency hopping (FH or FHSS)
  - Direct sequence (DS or DSSS)
  - Orthogonal Frequency Division Multiplexing (OFDM)
- Frequency-hopping systems
  - jump from one frequency to another in a random pattern, transmitting a short burst at each subchannel.
    - 2-Mbps IEEE 802.11 FH PHY
    - The cheapest to make : precise timing is needed to control the frequency hops, but sophisticated signal processing is not required to extract the bit stream
- Direct-sequence systems
  - spread the power out over a wider frequency band using mathematical coding functions.
  - 2-Mbps IEEE 802.11 DSSS PHY,
  - IEEE 802.11b HR/DSSS PHY.
  - require more sophisticated signal processing, which translates into more specialized hardware and higher electrical power consumption.
- OFDM
  - divides an available channel into several subchannels
  - encodes a portion of the signal across each subchannel in parallel
  - IEEE 802.11a, specifies the OFDM PHY.
  - IEEE 802.11g, specifies the ERP PHY, (operating at a lower frequency).

Principe de l'étalement de spectre

- L'étalement du spectre et sa recomposition



- L'étalement de spectre en présence de bruit

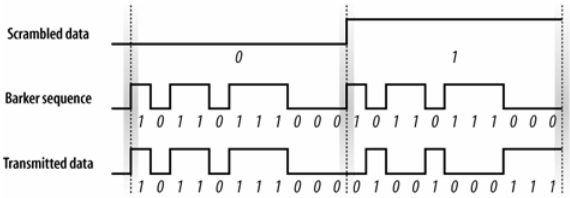


DSSS

- "Direct sequence spectrum spreading" :
  - La suite de bits est codée en une suite de bribes ("chips")
  - Les bribes sont plus "longues"

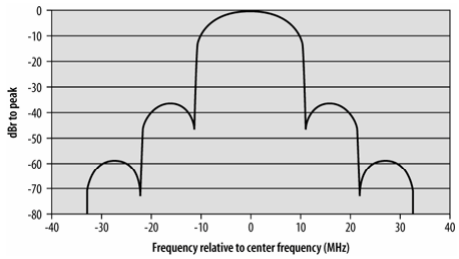
DSSS

- 802.11 uses the Barker sequence :
  - "10110111000"
  - 1 bit => 11 bits
  - Aussi appelée "scrambling", "randomization"



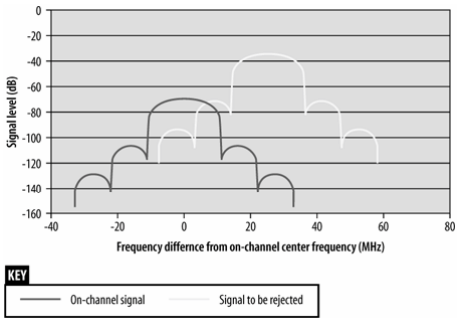
Etalement de l'énergie de DSSS

- L'énergie
  - exprimée sur une échelle logarithmique :
    - 30 db = 1/1000e
  - autour de 22 MHz



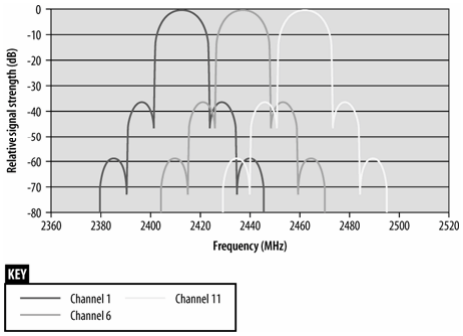
Etalement de l'énergie de DSSS

- Le niveau d'énergie du signal d'une autre canal ajacent sera plus faible et donc il sera écarté



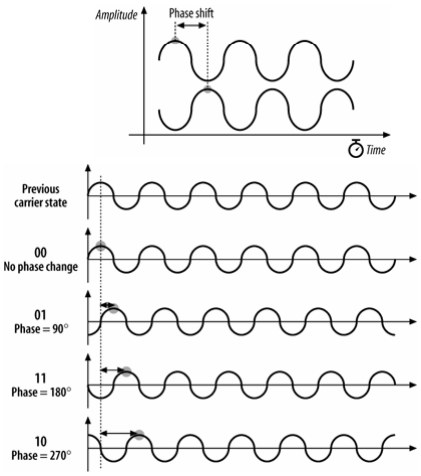
Canaux DSSS

- The DS PHY has 14 channels
  - In the 2.4-GHz band, each band is shitted by 5 MHz.
  - Channel 1 is placed at 2.412 GHz, channel 2 at 2.417 GHz, and so on up to channel 13 at 2.472 GHz
- Trois bandes de fréquences sans interférence entre leur premier lobe :
  - 5 * 5 Mhz > 22 Mhz



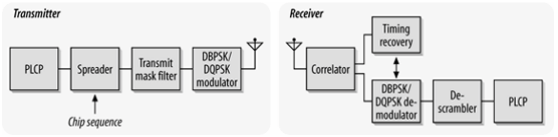
DPSK

- Differential Phase Shift Keying
  - Binary DPSK
  - QDPSK
- Q versus BPSK
  - Plus haut débit
  - Plus sensible aux interférences ("multipaths")
- DPSK versus PSK
  - Plus facile à décoder, meilleure sensibilité



DS PMD sublayer

- Exemple



CS/CCA for DS PHY

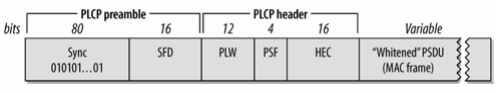
- Carrier Sense/ Clear Channel Assessment
  - Received energy detection > threshold (transmit power) => channel is busy
  - PLCD trame detected

Paramètres de la sous-couche DS PHY

Parameter	Value	Notes
Slot time	20 ms	
SIFS time	10 ms	The SIFS is used to derive the value of the other interframe spaces (DIFS, PIFS, and EIFS).
Contention window size	31 to 1023 slots	
Preamble duration	144 ms	Preamble symbols are transmitted at 1 MHz, so a symbol takes 1 ms to transmit; 144 bits require 144 symbol times.
PLCP header duration	48 ms	The PLCP header is 48 bits, so it requires 48 symbol times.
Maximum MAC frame	4096-8191 bytes	
Minimum receiver sensitivity	-80 dBm	
Adjacent channel rejection	35 dB	

"Whitened PSDU"

- Before transmission, the Physical layer whitens the PSDU by stuffing special symbols every four octets to minimize DC bias of the data signal. The PSDU whitening process involves the use of a length-127 frame-synchronous scrambler and a 32/33 bias-suppression encoding algorithm to randomize the data.



IEEE 802.11
La couche Liaison de Données

La couche Liaison de Données de l'IEEE 802.11

- Composée de 2 sous-couches
  - LLC : Logical Link Control
    - Offre les mêmes fonctionnalités quelque soit la sous-couche MAC : émission et transmission d'une trame
    - Facilite l'interconnexion d'un WLAN à tout autre réseau local appartenant à un standard de l'IEEE
  - MAC : Medium Access Control
    - Spécifique à l'IEEE 802.11
    - Dépende de la technologie de modulation et de codage
    - Similaire à la couche MAC de l'IEEE 802.3 du réseau Ethernet (c.-à-d. CSMA/CD)

Medium Access Control

Functionality:
- Reliable data delivery
- Fairly control access
- Protection of data

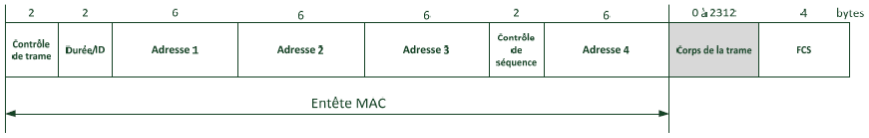
Deals:
- Access to a shared medium
- Noisy and unreliable medium => Physical layer
- Frame exchange protocol - ACK
- Overhead to IEEE 802.3
- Hidden Node Problem – RTS/CTS
- Participation of all stations
- Reaction to every frame

Les mécanismes de base

- Basic Access Mechanism
  - CSMA/CA
  - Binary exponential back-off
  - NAV : Network Allocation Vector
- Timing Intervals: SIFS, Slot Time, PIFS, DIFS, EIFS
- Retry Counters
  - Short retry counter
  - Long retry counter
  - Lifetime timer
- DCF Operation
- PCF Operation

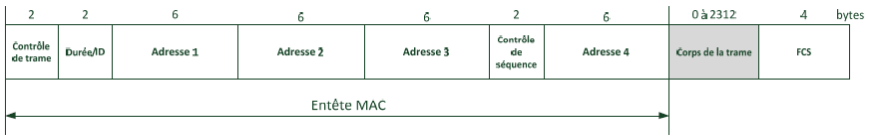
Format général d'une trame

- Les trames MAC sont constituées d'un en-tête, d'un corps et d'un FCS (*Frame Check Sequence).*
  - Le corps de la trame contient les données.
  - Le champ de contrôle de l'entête de la trame contient des informations telles que le protocole utilisé et le type de trame transmise.
  - Le champ "durée/ID" contient la durée de la transmission de la trame.
    - Cette valeur dépend du codage de la couche Physique et de la longueur de la trame.



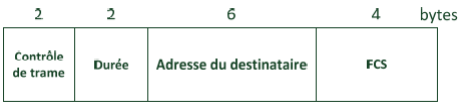
Format d'une trame de données

- Les champs "adresse" contiennent respectivement :
  - l'adresse du destinataire des données contenues dans le corps du paquet
  - l'adresse de la source des données contenues dans le corps du paquet
  - l'adresse de la station à laquelle cette trame est envoyée
    - lorsque la trame doit transiter par des relais avant d'atteindre sa destination
  - l'adresse de la station expédiant la présente trame
    - lorsque cette station est une station relais
- Le champ de contrôle de sequence
  - stocke le numéro de la trame
  - le numéro de fragment (si les données ont été fragmentées en plusieurs trames).



Trame d'acquittement

- La trame d'acquittement (ACK : "*Acknowledgement")*
  - Elle permet à l'émetteur d'une trame de s'assurer de sa bonne réception.
  - La valeur de l'adresse stockée dans le champ "Adresse du destinataire".
  - correspond à la valeur située dans le champ "Adresse 2" de la trame acquittée.



Champ "Control" de la trame IEEE 802.11

- **Version de protocole** : version du standard 802.11
- **Type et Sous-type** :
  - Le type de trame :
    - de gestion des services du réseau : gestion des associations, etc.
    - de contrôle : l'accès au média (ACK, RTS, CTS).
    - de données : contient les données des couches supérieures.
- **To DS** : la trame est destinée au système de distribution (DS)
  - Toute trame envoyée à destination d'un AP a un champ "To DS" positionné à 1.
- **From DS :** la trame provient du système de distribution (DS)
  - Lorsque les deux champs To et From sont positionnés à zéro, il s'agit d'une communication directe entre deux stations (mode ad hoc).

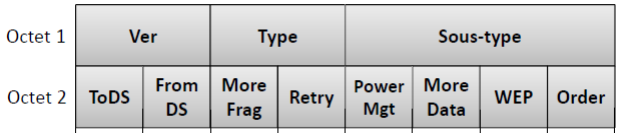
Octet 1	Ver		Type		Sous-type			
Octet 2	ToDS	From DS	More Frag	Retry	Power Mgt	More Data	WEP	Order

Champ "Control" de la trame IEEE 802.11

- **More Fragments :** indique qu'il reste des fragments à transmettre
- **Retry :** indique que le fragment en cours est une retransmission d'un fragment

précédemment envoyé

- **Power Management** : indique que la station entre en mode de gestion d'énergie
- **More Data** : utilisé par le AP pour indiquer à une station que des trames dont elle est destinatrice sonten attente.
- **WEP** : indique que l'algorithme de chiffrement WEP a été utilisé pour chiffrer le corps de la trame.
- **Order :** indique que la trame a été envoyée en utilisant la classe de service de livraison des trames de manière strictement ordonnée



Les trames de type de gestion des services d'IEEE 802.11

- Authentication frame:
  - 802.11 authentication begins with the WNIC sending an authentication frame to the access point containing its identity. With an open system authentication the WNIC only sends a single authentication frame and the access point responds with an authentication frame of its own indicating acceptance or rejection. With shared key authentication, after the WNIC sends its initial authentication request it will receive an authentication frame from the access point containing challenge text. The WNIC sends an authentication frame containing the encrypted version of the challenge text to the access point. The access point ensures the text was encrypted with the correct key by decrypting it with its own key. The result of this process determines the WNIC's authentication status.
- Association request frame:
  - sent from a station it enables the access point to allocate resources and synchronize. The frame carries information about the WNIC including supported data rates and the SSID of the network the station wishes to associate with. If the request is accepted, the access point reserves memory and establishes an association ID for the WNIC.
- Association response frame:
  - sent from an access point to a station containing the acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such an association ID and supported data rates.
- Beacon frame:
  - Sent periodically from an access point to announce its presence and provide the SSID, and other parameters for WNICs within range.
- Deauthentication frame:
  - Sent from a station wishing to terminate connection from another station.
- Disassociation frame:
  - Sent from a station wishing to terminate connection. It's an elegant way to allow the access point to relinquish memory allocation and remove the WNIC from the association table.
- Probe request frame:
  - Sent from a station when it requires information from another station.
- Probe response frame:
  - Sent from an access point containing capability information, supported data rates, etc., after receiving a probe request frame.
- Reassociation request frame:
  - A WNIC sends a reassociation request when it drops from range of the currently associated access point and finds another access point with a stronger signal. The new access point coordinates the forwarding of any information that may still be contained in the buffer of the previous access point.
- Reassociation response frame:
  - Sent from an access point containing the acceptance or rejection to a WNIC reassociation request frame. The frame includes information required for association such as the association ID and supported data rates.

Beacon frame

- Beacon frames are transmitted periodically to announce the presence of a Wireless LAN network.
  - Beacon frames are transmitted by the Access Point (AP), in an infrastructure BSS.
  - Beacon generation is distributed among the stations, in IBSS network.
- Beacon frame consist of MAC header, frame body and FCS. Main Beacon frame fields are:
  - Timestamp
    - After receiving the beacon frame all the stations change their local clocks to this time. This helps with synchronization.
  - Beacon interval
    - This is the time interval between beacon transmissions. Also known as Target Beacon Transmission Time (TBTT). It is a configurable parameter in the AP and typically configured as 100 TU.
  - Capability information
    - Capability information field spans to 16 bits and contain information about capability of the device/network. Type of network such as AdHoc or Infrastructure network is signaled in this field. Apart from this information, it announce the support for polling, encryption details also.
  - SSID
  - Supported rates
  - Frequency-hopping (FH) Parameter Set
  - Direct-Sequence (DS) Parameter Set
  - Contention-Free (CF) Parameter Set
  - IBSS Parameter Set
  - Traffic Indication Map (TIM)

  In the IEEE 802.11 standard, a unit of time (TU) equals to 1024 microseconds

SSID

- A **service set identifier** (**SSID**) is a name that identifies a particular 802.11 wireless LAN.
  - The SSID is defined as a sequence of 2–32 bytes.
    - As the SSID displays to users, it normally consists of human-readable characters. However, the standard does not require this.
  - A client device receives beacon messages from all access points within range advertising their SSIDs.
  - The client device can then either manually or automatically—based on configuration—select the network with which to associate.

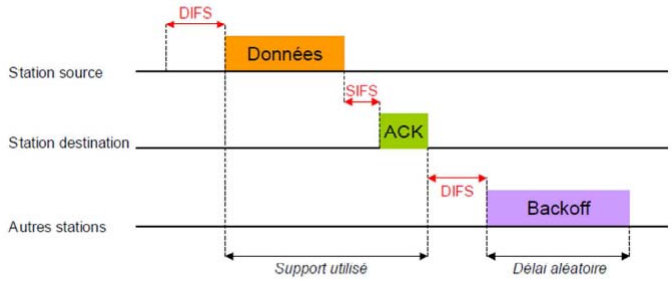
Principe du CSMA/CA

- Avant qu'une station n'émette :
  - elle vérifie au préalable que le canal de transmission n'est pas déjà occupé par une autre transmission.
    - La vérification de la disponibilité du canal s'effectue au moyen d'un mécanisme offert par la couche Physique. Ce mécanisme est appelé **CCA** (*Clear Channel Assessment).*
  - Si le canal est libre durant un DIFS, la station peut transmettre.
  - Dans le cas contraire, la station diffère sa transmission jusqu'à ce qu'elle détecte que le canal soit de nouveau libre.

Principe du CSMA/CA

- Lorsqu'une station envoie une trame
  - les autres stations mettent à jour un timer appelée **NAV** (Network Allocation Vector)
  - Le NAV permet de retarder toutes les transmissions prévues
    - NAV calculé par rapport à l'information située dans le champ durée de vie ou TTL contenu dans les trames envoyées
- Si la trame a été reçue correctement (après vérification du CRC de la trame),
  - la station de destination attend pendant un SIFS et émet un ACK
- Si l'ACK n'est pas détecté par la source (ou si la trame n'a pas été reçue correctement) on suppose qu'une collision s'est produite
  - la trame est retransmise.

Principe du CSMA/CA



Calcul du Backoff

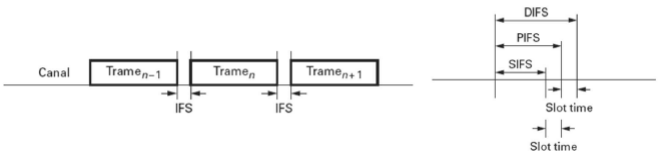
- Permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent transmettre des données en même temps
  - Temps découpé en tranches ("timeslots")
  - Le "timeslot" de 802.11 est un peu plus petit que la durée de transmission minimale d'une trame;
  - Utilisé pour définir les intervalles IFS
- Toutes les stations ont la même probabilité d'accéder au support
  - Chaque station doit, après chaque transmission d'une trame, réutiliser le même algorithme
- Inconvénient :
  - Pas de garantie de délai d'accès maximal
  - Rend difficile la prise en charge d'applications à contraintes temporelles (telles que la transmission de la voix ou de la vidéo)

Calcul du Backoff

- Initialement, la valeur du temporisateur "timer backoff" est compris entre 0 et 7
- Lorsque le canal est libre, les stations décrémentent leur temporisateur
- Si le canal est de nouveau occupé, la station bloque le temporisateur
- Dès que le temporisateur atteint 0,
  - la station transmet sa trame
  - Si le temporisateur de 2 ou plusieurs stations atteignent la valeur 0 au même instant, une collision se produit et chaque station doit recalculer une nouvelle valeur de leur temporisateur (comprise entre 0 et 15 lors de la deuxième tentative de retransmission)
- Pour chaque tentative de retransmission, la borne supérieur de l'intervalle du temporisateur croît de la façon exponentielle :
  - 2^(n+3)

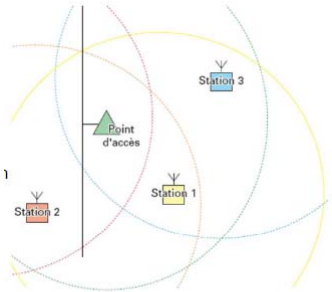
Inter Frame Space

- **SIFS** (*Short IFS)*
  - *utilisé pour la transmission des* trames d'acquittement et des rafales de trames issues d'une même station.
- **PIFS** (*PCF IFS)*
  - *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.
- **DIFS** (*DCF IFS)*
  - *utilisé en* mode DCF comme temps minimal d'attente avant transmission.
- **EIFS** (*Extended IFS)*
  - *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.



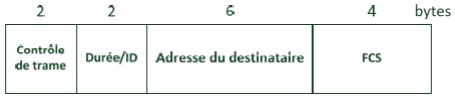
Gestion des stations cachées

- Le problème des stations cachées est propre au réseau sans fil.
- Exemple:
  - La station 1 peut écouter les stations 2 et 3.
  - Les stations 2 et 3 peuvent écouter la station 1, mais ne peuvent pas s'écouter entre elles.
  - Lorsque la station 2 transmet à la station 1 une trame, cette transmission n'est pas détectée par la station 3.
  - La station 3 peut alors décider de transmettre simultanément une autre trame perturbant la réception de la station 1.
- Pour éviter cette situation, un mécanisme d'annonce de transmission à été intégré.
  - Ce mécanisme utilise les trames RTS (*Ready To Send) et CTS (Clear To Send)* qui précèdent la transmission.



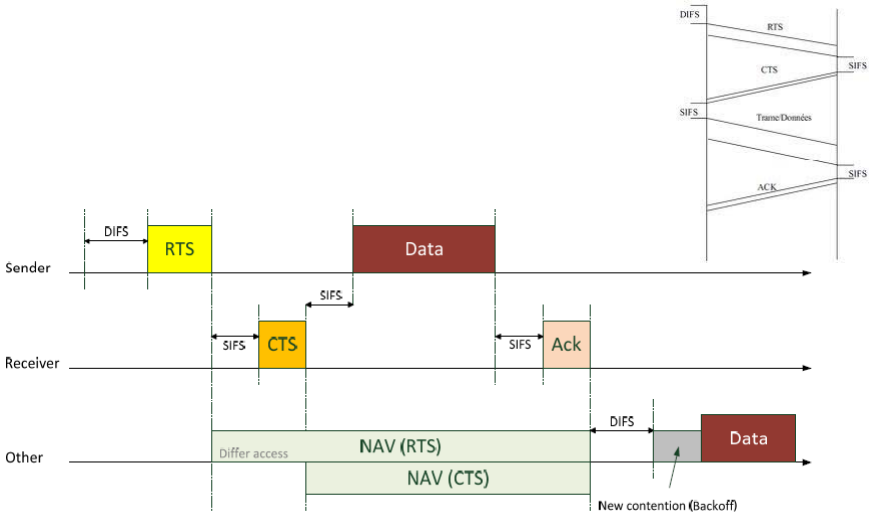
Format des trames RTS et CTS

Trame RTS



Trame CTS

Gestion des stations cachées



Gestion des stations cachées

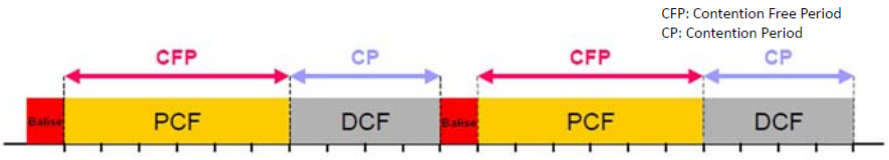
- Le mécanisme de gestion des stations cachées entraîne un surcoût important
  - transmission sur le canal des trames de signalisation, RTS et CTS
    - perte de bande passante
- Un mécanisme additionnel appelé "RTS_Threshold" tente de limiter leur surcoût.
  - Si la longueur des données à transmettre est inférieure à ce seuil, la transmission de trame de donnes se fera sans utilisation des trames RTS et CTS.
  - Si le seuil est dépassé alors le mécanisme de gestion des stations cachées (avec RTS/CTS) est utilisé pour la transmission.
- Ce mécanisme est le plus souvent non activé.

Deux modes de contrôle d'accès

- DCF (Distributed Coordination Function)
  - CSMA/CA (Carrier Sense Multiple Access/ Collision Avoidance)
  - Aucun contrôle centralisé
  - Toutes les implémentations doivent supporter ce mode
  - Offre un service similaire au réseau traditionnel supportant le Best Effort
    - Conçu pour prendre en charge le transport de données asynchrones
    - Tous les utilisateurs qui veulent transmettre ont une chance égale d'accéder au support
- PCF (Point Coordination Function)
  - L'AP supervise tout le trafic
  - Mode optionnel
  - Conçue pour la transmission de données sensibles au délai

Modes d'accès et types de réseau

- Réseau ad-hoc
  - Uniquement le mode DCF
- Réseau classique IEEE 802.11, avec des AP
  - À la fois les deux modes DCF et PCF
  - La séquence DCF/PCF est initialisée, par l'émission d'un balise par l'AP qui indique la durée de la phase PCF

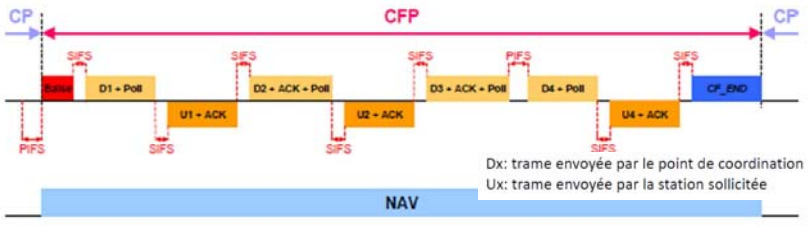


Le mode PCF

- Le mode PCF consiste en une gestion centralisée des ressources.
  - L'AP contrôle tout le trafic : il n'y a jamais de collisions
- C'est le point d'accès qui ordonne les transmissions et distribue le droit à la parole.
  - C'est par l'intermédiaire de trames d'administration spécifique qu'une sollicitation explicite est effectuée auprès d'une station pour lui attribuer le droit à émettre (mécanisme de polling)
- L'utilisation de la PCF est optionnelle et donc peu ou pas implémentée dans les matériels 802.11.

Le mode PCF

- L'AP accorde un temps de parole à chaque station.
- Si cette dernière en a besoin, elle émet un acquittement puis ses données.
- Si elle n'a pas répondu dans un délai court, la parole est passée à une autre station
- PCF peu efficace si la plupart des stations sont silencieuses.



Le mode DCF

- DCF is fundamental access method
- IFS : Inter-frame Spacing
  - SIFS< PIFS < DIFS < EIFS
  - IEEE 802.11n has introduced RIFS which is a smallest Inter-Frame spacing
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance
  - Look for activity,
    - if free,
      - wait (DIFS) and transmit if still free
    - If medium is busy,
      - random back-off a number of slots (min 15, max 1023)
      - Count down slots as long as medium is not busy
      - When count down is zero, transmit
        - if packet fails (e.g. collision), back-off with increased random window, up to a preconfigured upper limit

Le mode DCF

- Le mode DCF utilise un algorithme distribué pour gérer l'accès au canal.
  - L'algorithme CSMA/CA ("*Carrier Sense Multiple Access with Collision Avoidance")*
    - *La méthode CSMA/CA est basée sur une fonction de détection de porteuse pour déterminer si le médium est occupé ou non*
    - *Cette méthode nécessite également l'emploi de trou (d'absence de toute émission), d'une durée minimale spécifiée entre deux transmissions d'une trame. Il est appelé IFS ("Inter Frame Space").*
  - Il est complété par un tirage d'un délai aléatoire lorsqu'une station constate que le canal est occupé et avant transmission ("*exponential backoff").*

Economie d'énergie

- Les stations mobiles peuvent décider d'entrer dans un mode d'économie d'énergie

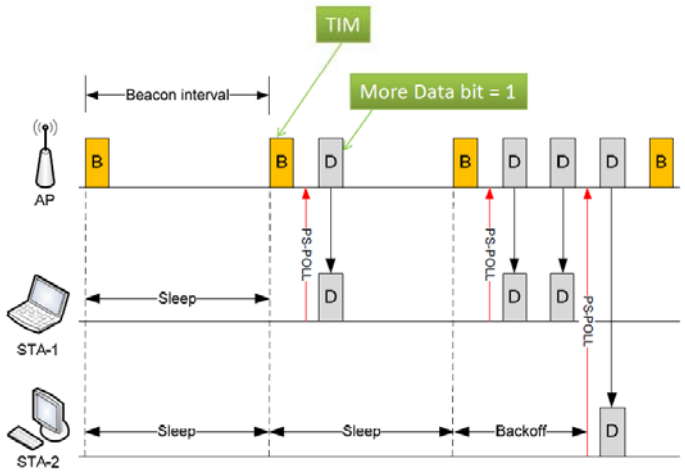
.

- Pendant ce temps, le point d'accès en charge de cette station mémorise les trames envoyées vers celle-ci, les conserve. Il les retransmettra lorsque celle-ci sera à nouveau disponible.

Le mode PSM ("Power Saving Mode")

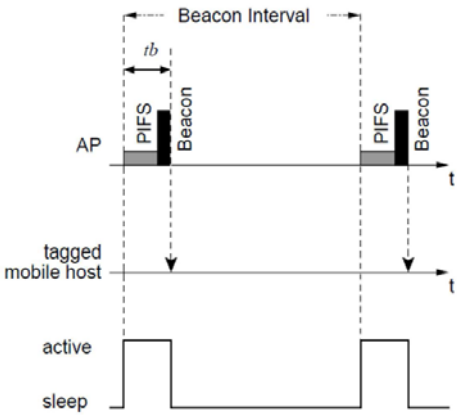
- Rôle du AP
  - Mémorisation des trames durant la mise en veille d'une station
  - Prévient chaque station de la disponibilité de trames à recevoir
    - Champ "Traffic Indication Map" (TIM)
    - Dans les trames "Beacon"
  - Annonce d'autres trames de données à suivre
    - Champ "More Data" (1 bit)
    - Dans les trames de données
- Rôle des STA
  - Envoi du PS-Poll à chaque trame à recevoir
    - Utilise le mode DCF
  - Se met en veille s'il n'y a pas de trames à recevoir ou à envoyer.

Le mode PSM ("Power Saving Mode")



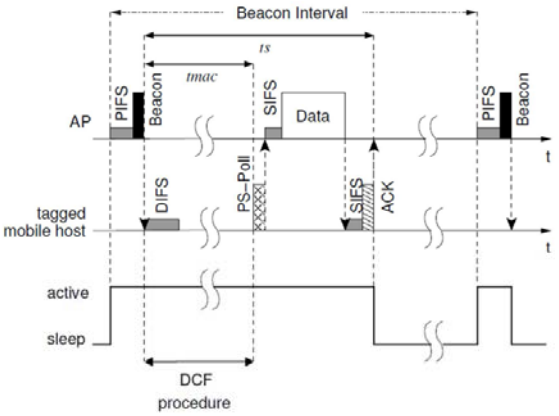
Le mode PSM ("Power Saving Mode")

- Une station peut s'endormir entre deux Beacons si elle n'a rien à recevoir (ni a émettre).
- Elle doit être réveillée pour interpréter chaque Beacon.



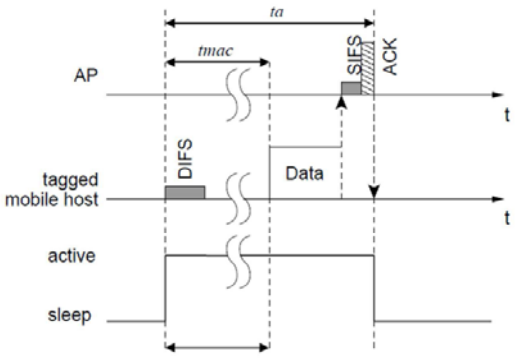
Le mode PSM ("Power Saving Mode")

- Réception d'un trame par une station.



Le mode PSM ("Power Saving Mode")

- Emission d'un trame par une station.



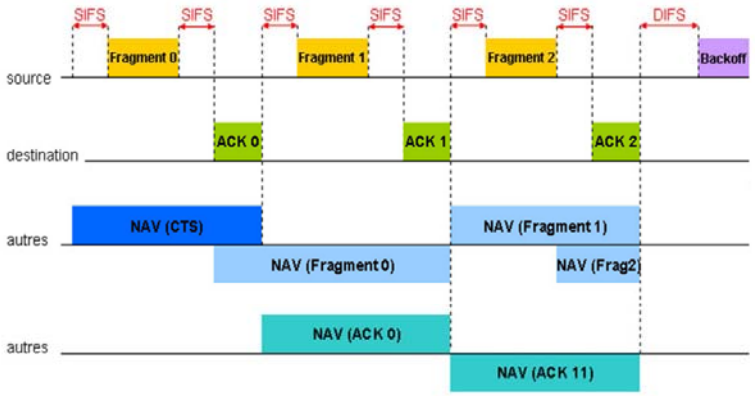
Le mode PSM ("Power Saving Mode")

- Avantages
  - Économise l'énergie, en se mettant en veille, s'il n'y a pas de paquets à recevoir (ni à émettre)
  - Utilise le mode DCF
- Inconvénients
  - Les mobiles gérés en mode PSM doivent être synchronisés avec le point d'accès pour la réception des "Beacons"
  - Réveil à chaque envoi d'un "Beacon"
    - Temps de calcul de la période de mise en veille assez difficile

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 dans de nombreux cas
  - Augmente les performances globales du réseau
- Fragmentation utilisée dans les liaisons radio, dans lesquelles le taux d'erreur est important
  - Plus la taille de la trame est grande et plus elle a de chances d'être corrompue
- Quand une trame est fragmentée, tous les fragments sont transmis de manière successive
  - Le canal 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 retransmettre 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

Fragmentation – réassemblage



Hand-over

- Le standard IEEE 802.11f adresse la problématique du Handover et du Roaming
- Le Handover permet le passage d'une cellule à une autre sans interruption de la communication
  - Se fait entre 2 transmissions de trames et non au milieu d'un dialogue
- Lorsque les terminaux se déplacent, ils doivent rester synchronisés pour pouvoir communiquer
  - Lors de la réception d'un beacon, les stations mettent à jour leurs horloges pour rester synchronisées avec le point d'accès
- Lorsqu'une station se déplace physiquement par rapport à son point d'accès d'origine, elle provoque une réassociation
  - Diminution de la puissance du signal
  - Equilibrage de charge au sein d'un BSS ou ESS ("Load balancing")

Conclusion

- Les techniques de transmission sans fil
  - IEEE 802.11 (wifi)
  - Couche Physique
    - Techniques de modulation adaptés à un environnement variable
  - Couche Liaison de Données
    - Gestion de l'accès au CSMA/CD
    - Résolution du problème de la station cachée
    - Deux mode opératoires DCF, PCF
    - Mode d'économie d'énergie
  - De nombreuses variantes et extensions
    - Plus de débit => IEEE 802.11g
    - Gestion de la QoS
    - Meilleure gestion de la sécurité du canal radio
    - Gestion du "roaming"
    - Etc.