Les réseaux 802.11

Les réseaux 802.11 : Plan

- Introduction
- Architecture
- Couche Physique
- Couche liaison

Introduction

- Les réseaux *wireless* «mobiles» sont des réseaux qui utilisen l'interface radio comme support de transmission.

ntérêt de l'interface radio :

- Couper le cordon ombilicale qui relie un téléphone, un fax, u PC ➔ mobilité du terminal et/ou usager

Contrepartie (Spécificités du médium de transmission)

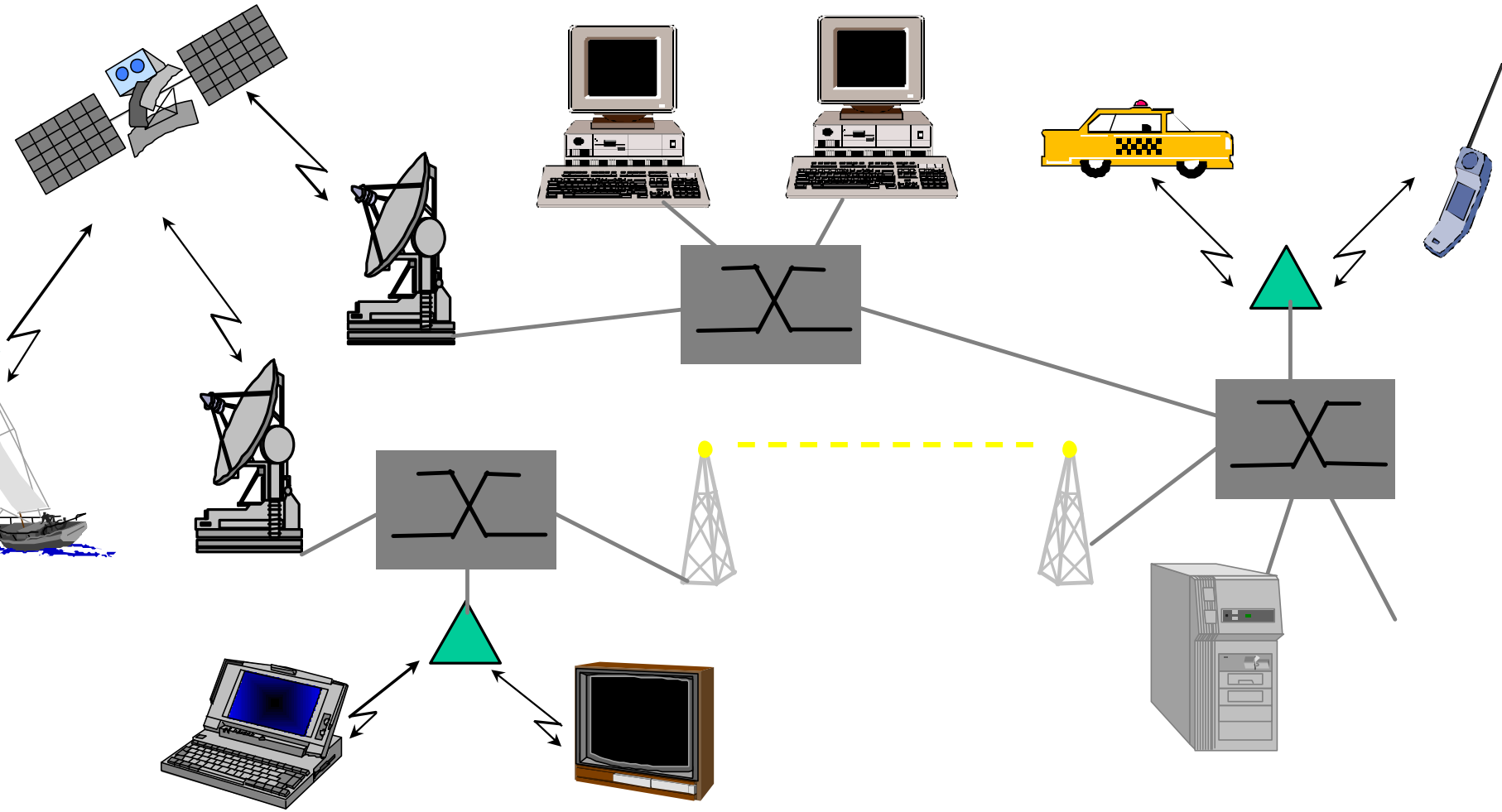
- commun à tous les utilisateurs et «diffusif»(possibilité d'écoute indiscrètes)
- canal perturbable par des interférences,
- phénomènes variables dans l'espace et le temps
- le médium est rare et donc coûteux

Introduction

- Les réseaux « wireless » peuvent être classés selon différents critères:
  - Mobilité : réseaux de mobiles /sans fil ; (*)
  - Type de transmission voix/données ;
  - Terrestres/satellites.

- Mobilité :
  - Réseau de mobiles : permet de se déplacer à travers le réseau en conservant une même adresse et propose un accès sans fil à l'information (GSM, IP-mobile).
  - Réseau sans fil : communication hertzienne sur une zone géographique restreinte en taille (téléphone sans cordon).

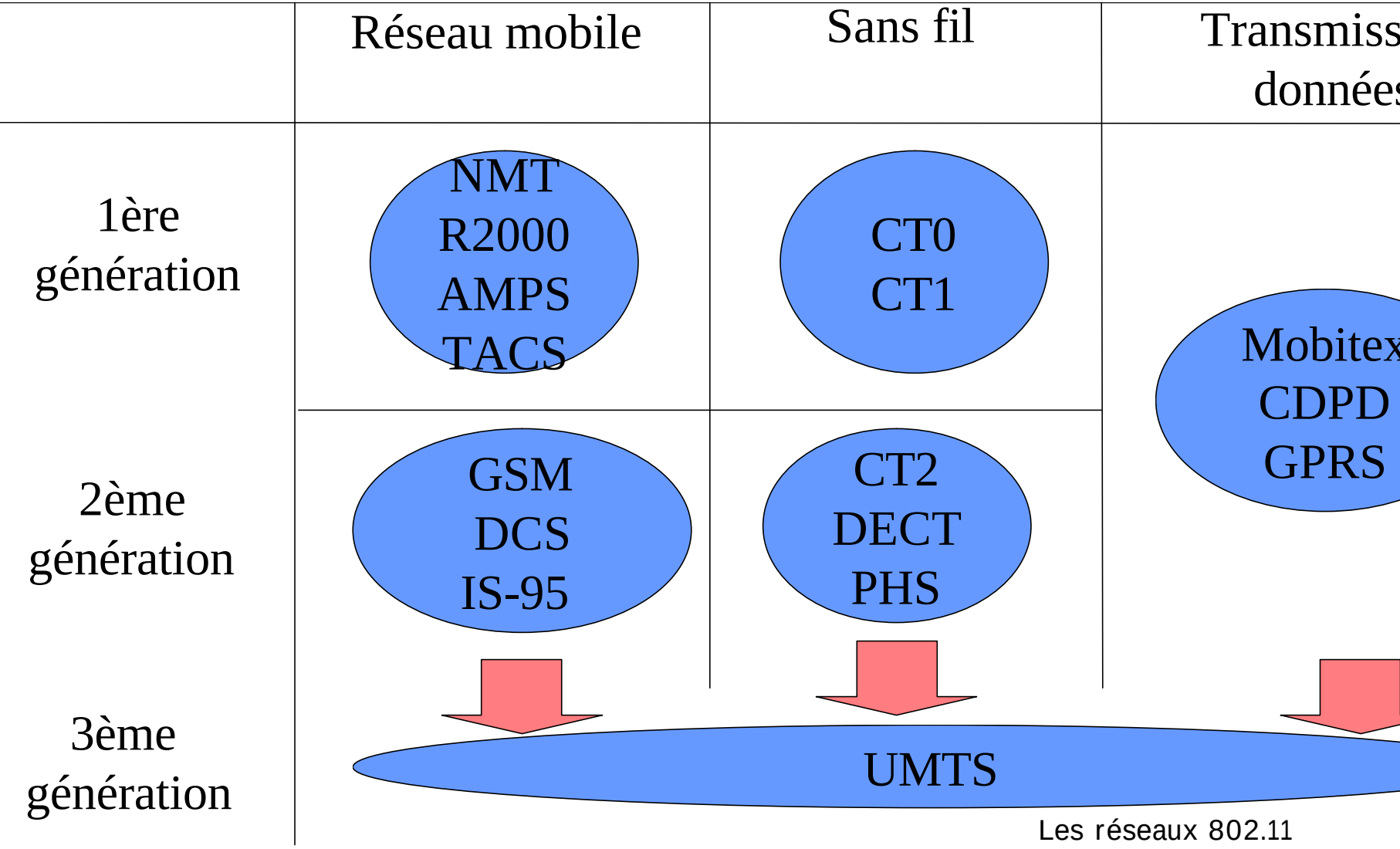
Quelles applications ?



Évolution des systèmes mobiles

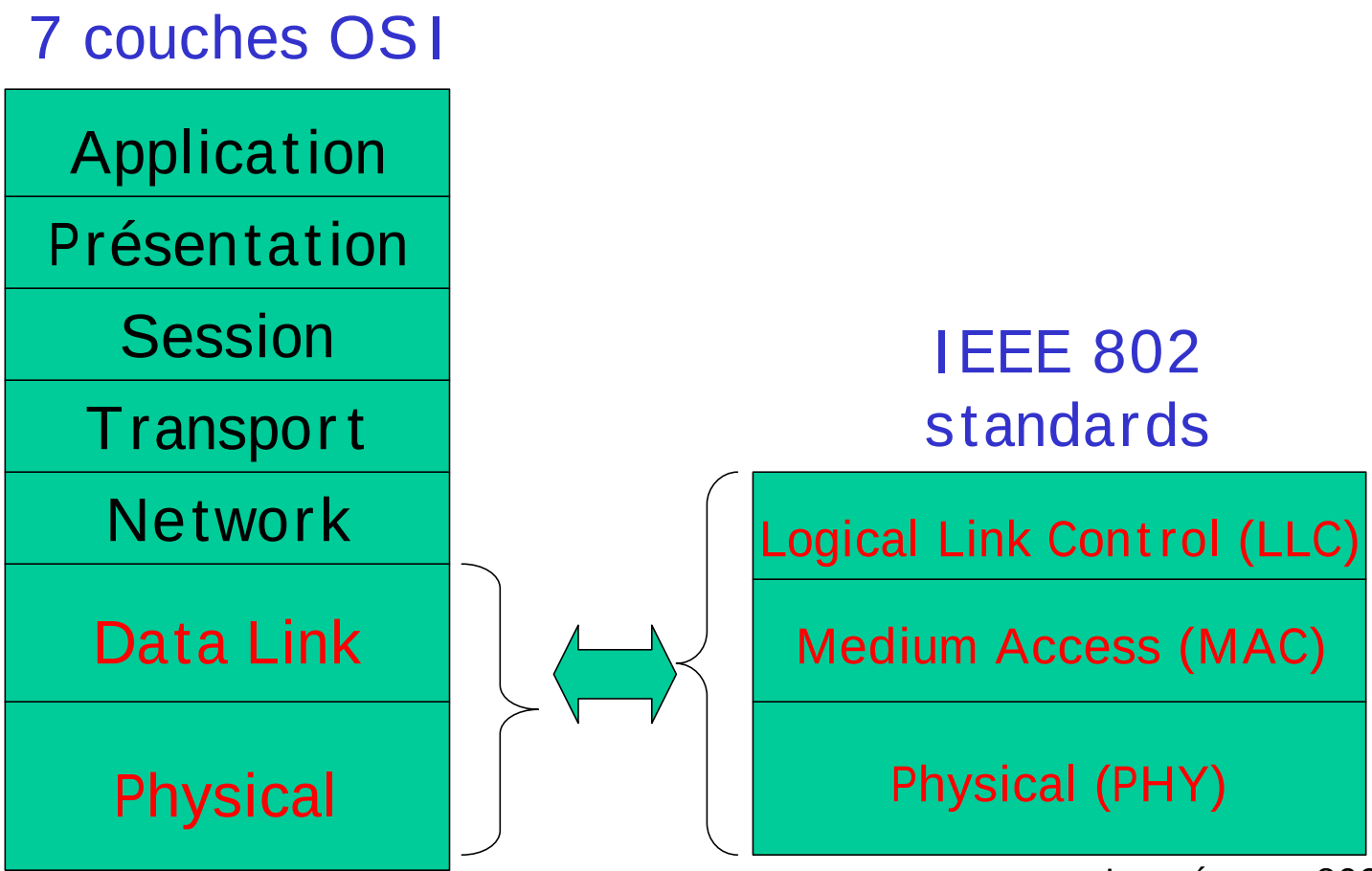
- 1ère génération (1G) :
  - Transmission analogique
  - Contrôle numérique
  - Concept de cellule
- 2ème génération (2G) :
  - Transmission et contrôle numérique
  - Concept de cellule
- 2G+ : GPRS
- 3ème génération (3G) : UMTS/IMT-2000
  - Un seule système pour la voix et les données
- 4ème génération (4G) : plus …

Evolution des systèmes mobiles



IEEE 802.11 : Normalisation

- Les réseaux locaux 802.11 sont normalisés par IEEE.



Le standard IEEE 802.11

- **802.11** - Standard d'origine (juin 1997)
  - Le groupe de travail concentre maintenant ses efforts pour produire des standards pour des WLAN à grande vitesse

- **802.11x** – Amendements

  - **802.11b** - Vitesse de 11 Mbits/s (bande ISM)
  - **802.11a** - Vitesse de 54 Mbits/s (bande UN-II)
  - **802.11g** - Vitesse de 54 Mbits/s (bande ISM)
  - **802.11e** - Qualité de service
  - **802.11i** - Amélioration de la sécurité
  - **802.11f** - Roaming

Le standard IEEE 802.11

But
- connectivité sans fil à des stations fixes/mobiles
- Déploiement rapide
- Utilisation de différentes bandes de fréquences

- Standard d'origine

Définis :

- La sous couche MAC
- 3 couches physique (PHY)
  - IR (Infrarouge)
  - FHSS (Frequency Hopping Spread Spectrum)
  - DSSS (Direct Sequence Spread Spectrum)

Remarques :

- FHSS et DSSS utilisent la bande des 2,4/2,483 Ghz de l'ISM (Industrial, Scientific and Medical): Uitilsation libre dans de nombreux pays
- Ajout de 2 couches physique (amendements)

Famille IEEE 802.11

- 802.11b (WiFi)
  - 2.4-5 GHz (sans license)
  - Jusqu'à 11 Mb/s
  - DSSS
  - Largement déployé
- 802.11a
  - 5-6 GHz
  - Jusqu'à 54 Mb/s
- 802.11g
  - 2.4-5 GHz range
  - Jusqu'à 54 Mb/s

Les lois de la Radio :
Débit plus grand = Couverture plus faible
Puissance d'émission élevée = Couverture plus grande,
mais durée de vie des batteries plus faible
Fréquences radio élevées = Meilleur débit, couverture plus faible

Les réseaux 802.11 : Plan

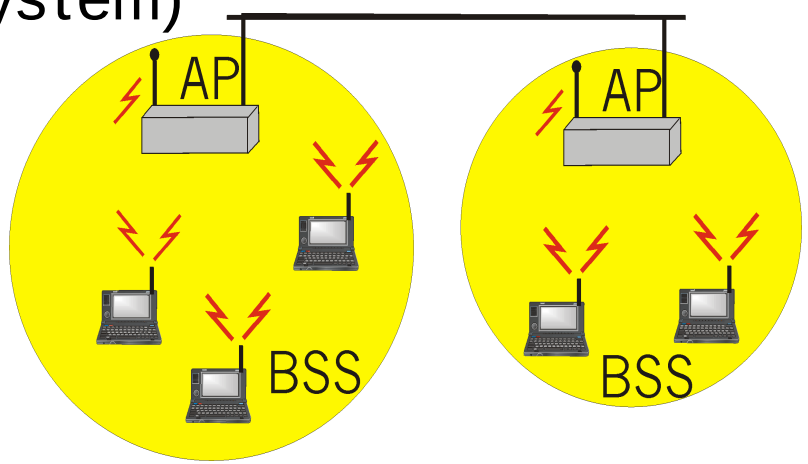
- Introduction
- Architecture
- Couche Physique
- Couche liaison

Architecture

- Deux modes de fonctionnement
  - Mode infrastructure
  - Mode ad hoc (peer-to-peer)

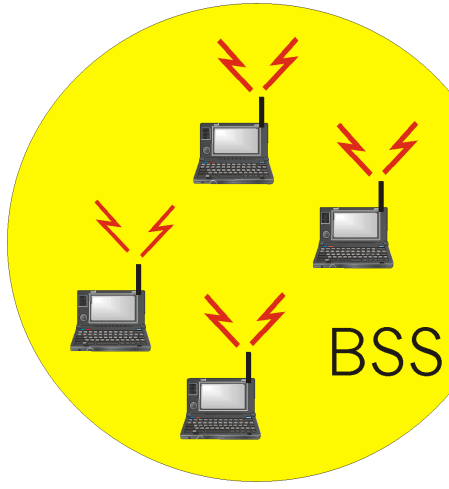
Mode Infrastructure

- Les stations mobiles communiquent avec une station de base
  - Station de base = point d'accès (AP : access point)
- Basic Service Set (BSS) (cellule) contient:
  - Stations mobiles
  - Un point d'accès (AP): station de base
- Les BSS sont reliés par un système distribué (DS : distribution system)



Mode Ad Hoc

- Pas de AP (station de base)
- Les stations mobiles communiquent entres elles
  - Les paquets de la station A vers la station B peuvent avoir besoin de transiter par les hôtes X, Y, Z
- Applications:
  - Conférences, train, bus …
  - Domicile : interconnection d'équipement personnel (ordinateurs, imprimante, …)
  - …
- IETF MANET
  (Mobile Ad hoc Networks)
  groupe de travail

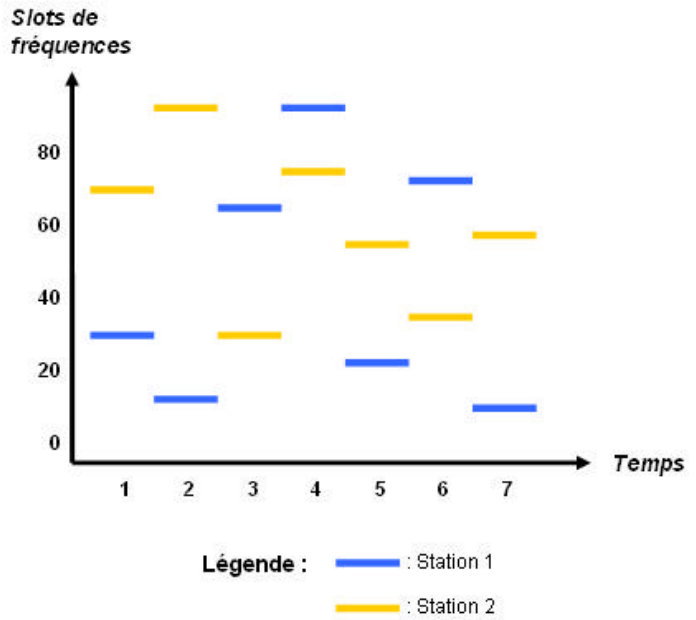


Les réseaux 802.11 : Plan

- Introduction
- Architecture
- Couche Physique
- Couche liaison

FHSS : Principe

- Bande ISM : 2,4/2,483 GHz
- 79 canaux disjoints de 1 Mhz
- Débit : 1 ou 2 Mb/s
  - Données rapides → taux d'erreurs élevé
- Utilise un changement de fréquence syncrhronisé toute les 0,4 s
- Négociation du schéma de transmission (Hopping Pattern)

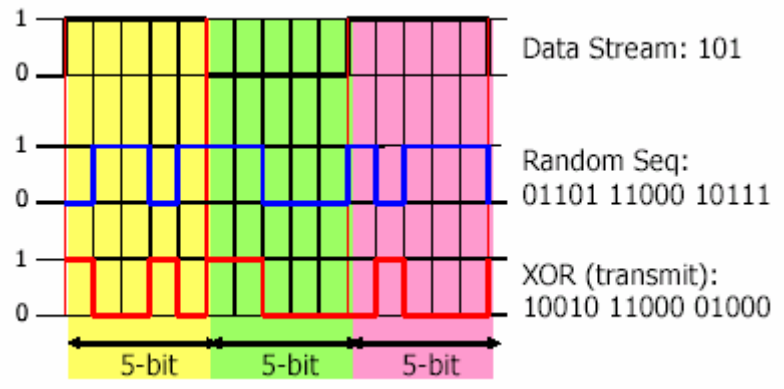


Performances

- Coût bas
- Petite consommation d'énergie
- Bonne tolérance aux bruits
- Débit faible

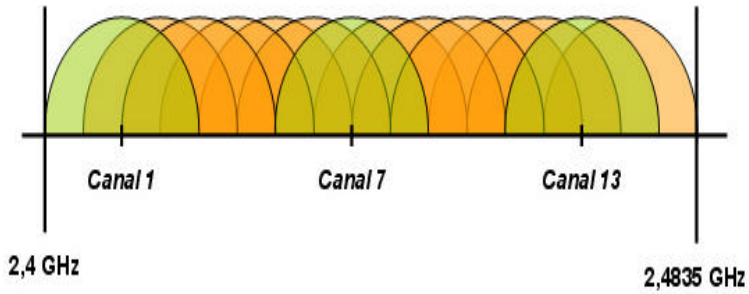
DSSS : Principe

- Bande ISM : 2,4/2,483 GHz
- Débit : 1, 2, 5.5, 11 Mb/s
- Un bit → plusieurs bits (11)
- Transmission des données XOR une séquence de bits Chipping Code



Performances

- Coût élevé
- Consommation d'énergie importante
- Débit important
- Redondance bits → diminution des retransmission



Les réseaux 802.11 : Plan

- Introduction
- Architecture
- Couche Physique
- Couche liaison

Couche liaison de données

Composée de 2 sous-couches

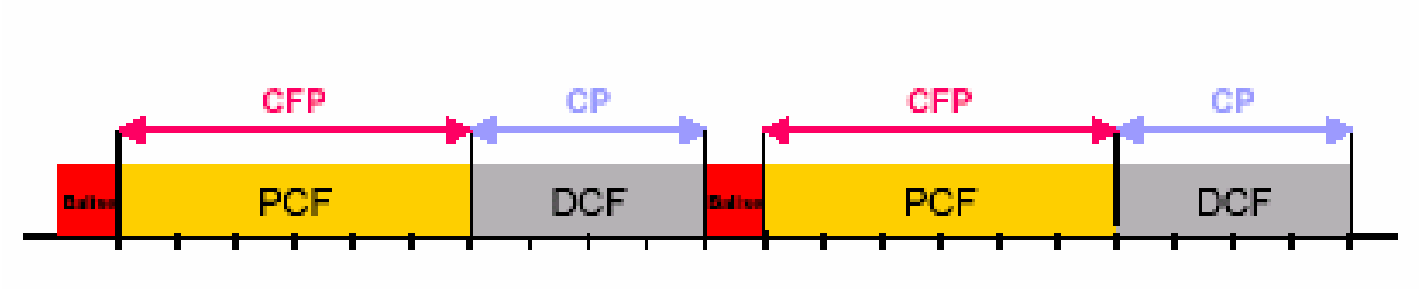
- LLC : Logical Link Control
  - Utilise les mêmes propriétés que la couche LLC 802.2
  - Possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE

- MAC : Medium Access Control
  - Spécifique à l'IEEE 802.11
  - Assez similaire à la couche MAC 802.3 du réseau Ethernet terrestre

Accès au médium

La couche MAC définis :

- 2 méthodes d'accès au support:
  - Mécanisme de base : DCF (Distributed Coordination Function)
  - Mécanisme optionnel : PCF (Point Coordination Function)



- Mode ad-hoc
  - Uniquement DCF
- Mode infrastructure (avec points d'accès)
  - DCF et PCF

DCF

- Basé sur le protocole CSMA/CA (Carrier Sense MultipleAccess/Collision Avoidance)
- CSMA :
  - Offre toute la bande passante si une station transmet seule
  - Ne transmet pas si une transmission est en cours
  - Ne détecte pas de collision en cours de transmission
- CA :
  - mécanisme d'éviter des collisions

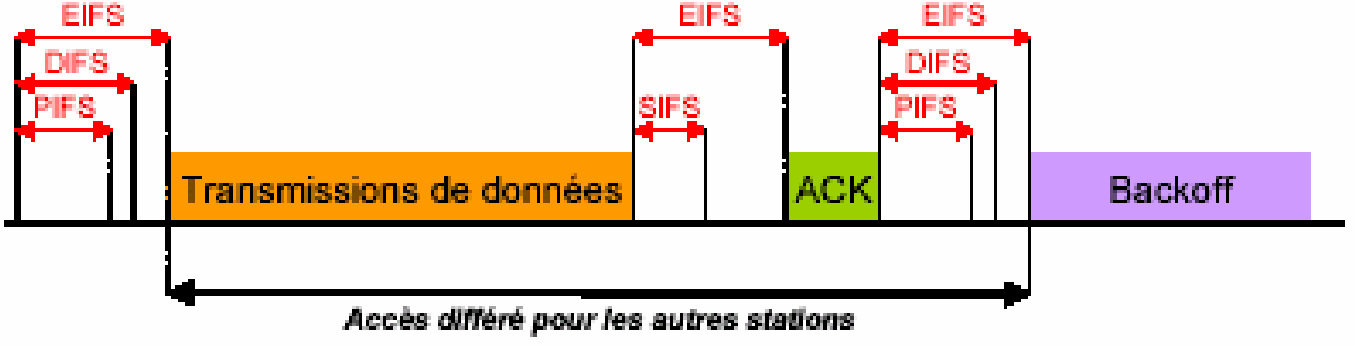
- Ethernet : CSMA/CD (Collision Detection)
  - CSMA/CD ne peut pas être utilisé dans les environnements sans fil

- Détection de collision : une station doit être capable d'écouter et de transmettre en même temps
  - Systèmes radio : la transmission couvre la capacité de la station à entendre la collision
  - Si collision : la station continue à transmettre la trame complète (perte de performance du réseau)

CSMA

Le CSMA est basé sur :

- L'écoute du support
- L'utilisation d'acquittements positifs
- L'algorithme de Backoff
- 4 type de temporisateurs IFS : **SIFS, PIFS, DIFS, EIFS**
  - Intervalles IFS = périodes d'inactivité sur le support de transmission
  - Intervalle de temps entre la transmission de 2 trames
  - Permet d'instaurer un système de priorités (+ le délais est petit + l'accès est prioritaire)



CSMA

802.11 CSMA: émetteur

- si le canal est libre pendant **DISF** sec.

  alors transmission de la trame entière (pas de détection de collision)

- si le support est occupé

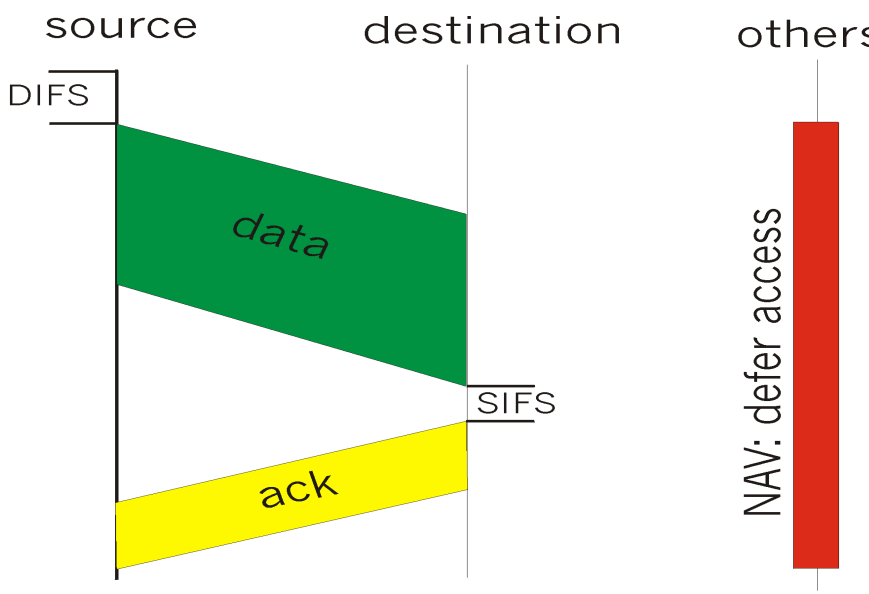
  alors binary backoff

802.11 CSMA récepteur

- si la réception est correct

  alors transmission d'un ACK après **SIFS** sec.

  (ACK nécessaire : problème de la station cachée)



Algorithme de backoff

- Permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent transmettre des données en même temps

- Fonctionnement :
  - Temps découpé en Timeslot
  - Fenêtre de contention : CW (CWmin = CW = CWmax)
  - Une station écoute le support avant toute tentative de transmission
    - Si le support est libre après un DIFS : transmission
    - Sinon elle calcule un temporisateur suivant la formule : ***TBACKOFF = random (0, CW) x Timeslot***
    - Chaque fois que le support est libre, ***TBACKOFF*** est décrémenté de 1.
    - Dès que ***TBACKOFF*** atteint la valeur 0, la trame est émise.

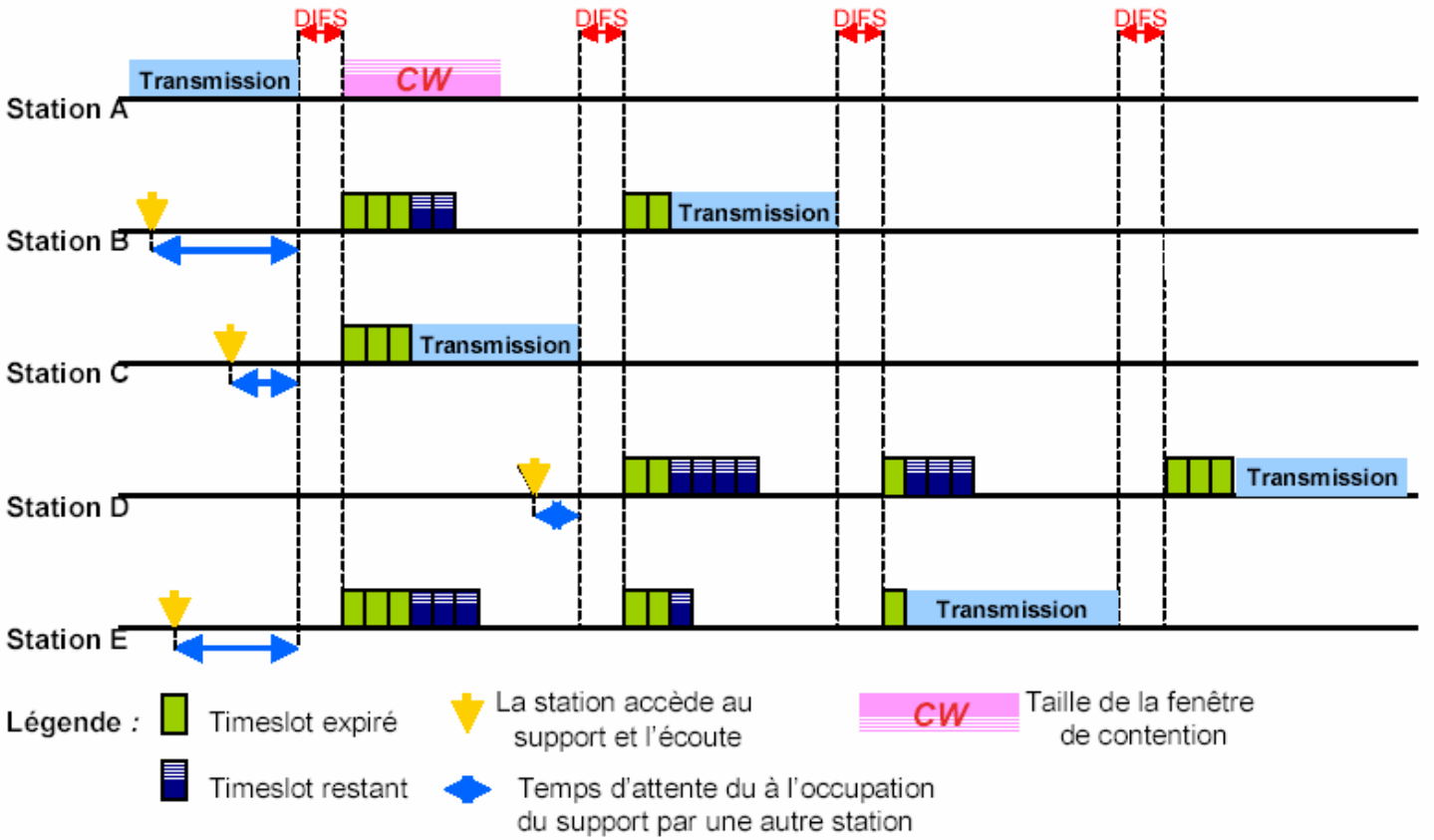
  - Il y a collision lorsque :
    - Deux stations ont la même valeur de temporisateur
    - Un ACK n'est pas reçu par l'émetteur
    - A chaque collision, la taille de la fenêtre de contention (CW) double

Algorithme de backoff

- Les stations ont la même probabilité d'accéder au support car chaque station doit, après chaque retransmission, réutiliser le même algorithme

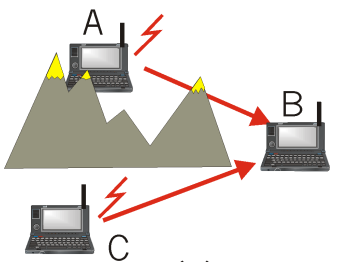
- Inconvénient :
  - pas de garantie de délai minimal
  - Complique la prise en charge d'applications temps réel telles que la voix ou la vidéo

Algorithme de backoff

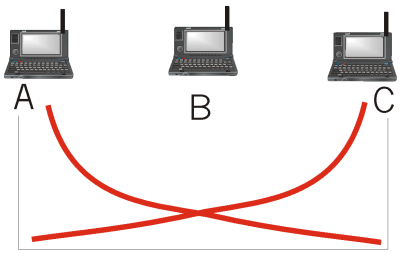


Collision avoidance (CA)

- Problème de la station cachée:
  - Deux stations situées chacune à l'opposé de l'AP ou d'une autre station
  - Ne peuvent pas s'entendre mutuellement pour cause de distance ou de présence d'obstacles
  - Effectuent des transmissions : Bande passante perdue !
- Solution:
  - Réservation du support trames : RTS/CTS
  - Etat du support : NAV (network allocation vector)



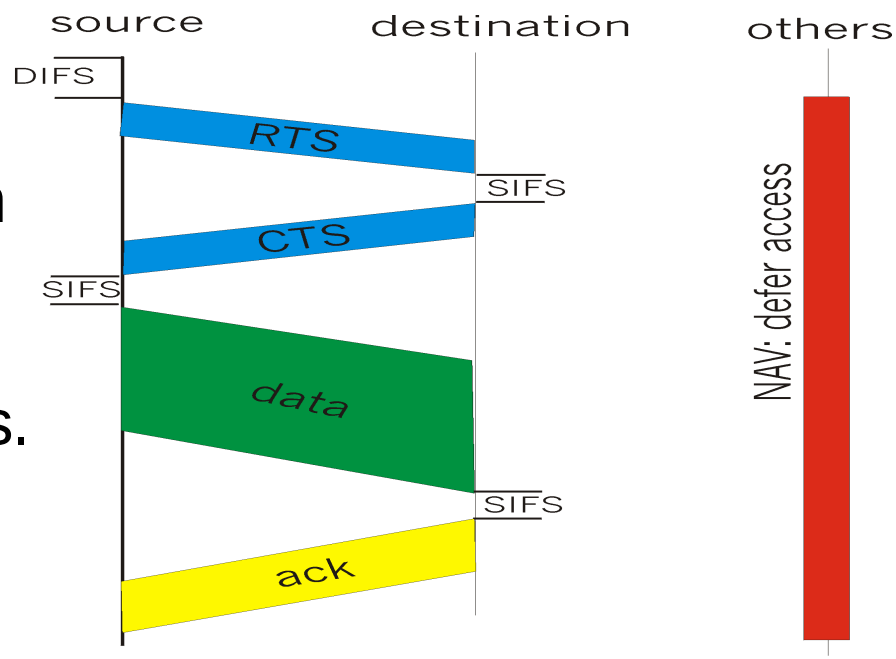
(a)



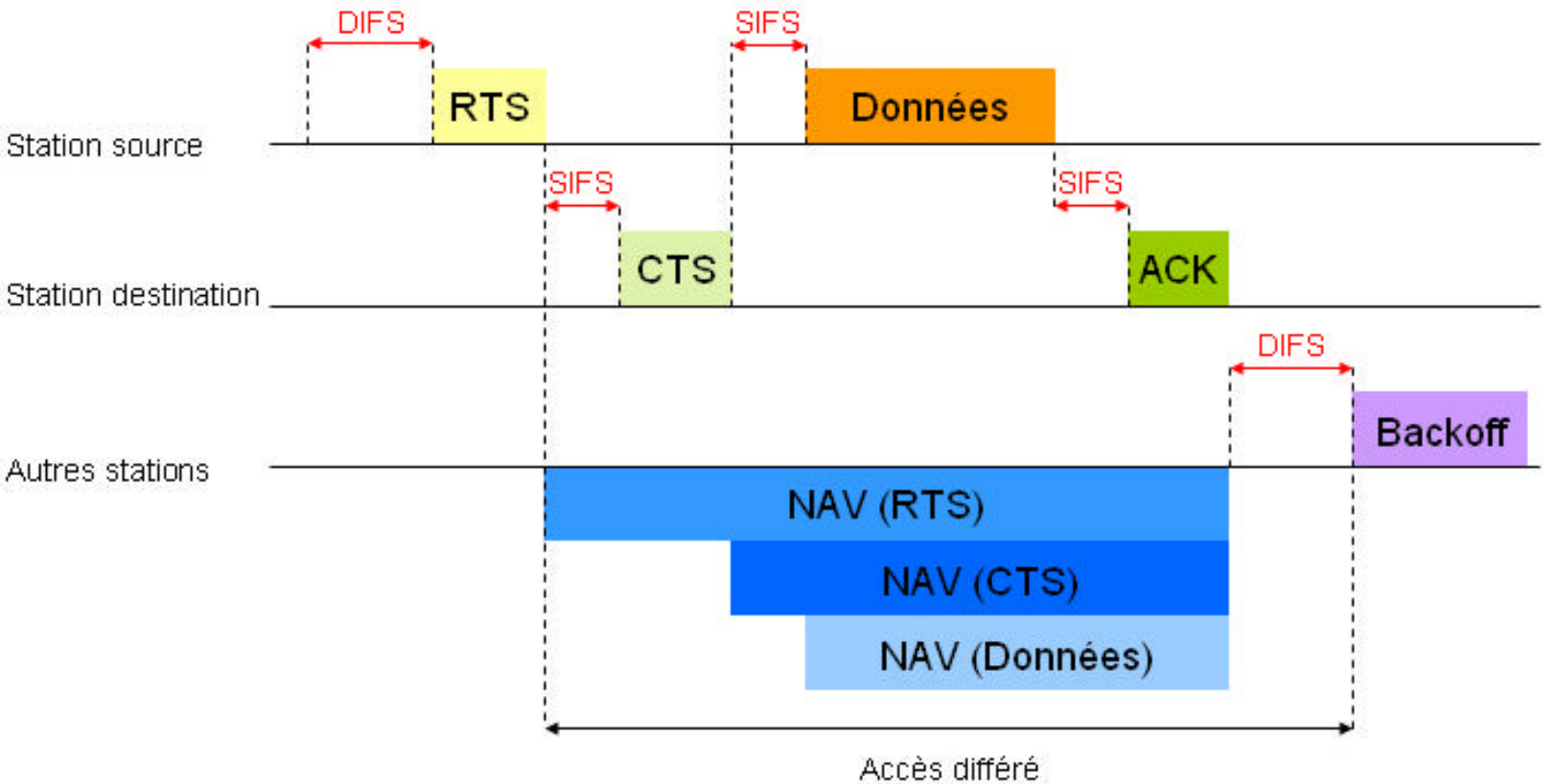
(b)

Echange : RTS-CTS

- Emetteur transmet un petit paquet RTS (request to send) : indiquant l'émetteur le récepteur et la durée de la transmission
- Récepteur répond avec un petit paquet CTS (clear to send) avec les mêmes infos.
- Autres stations :
  - mettent à jour leur NAV avec les informations du RTS-CTS
  - Ne transmettent pas pendant la durée spécifiée par le NAV



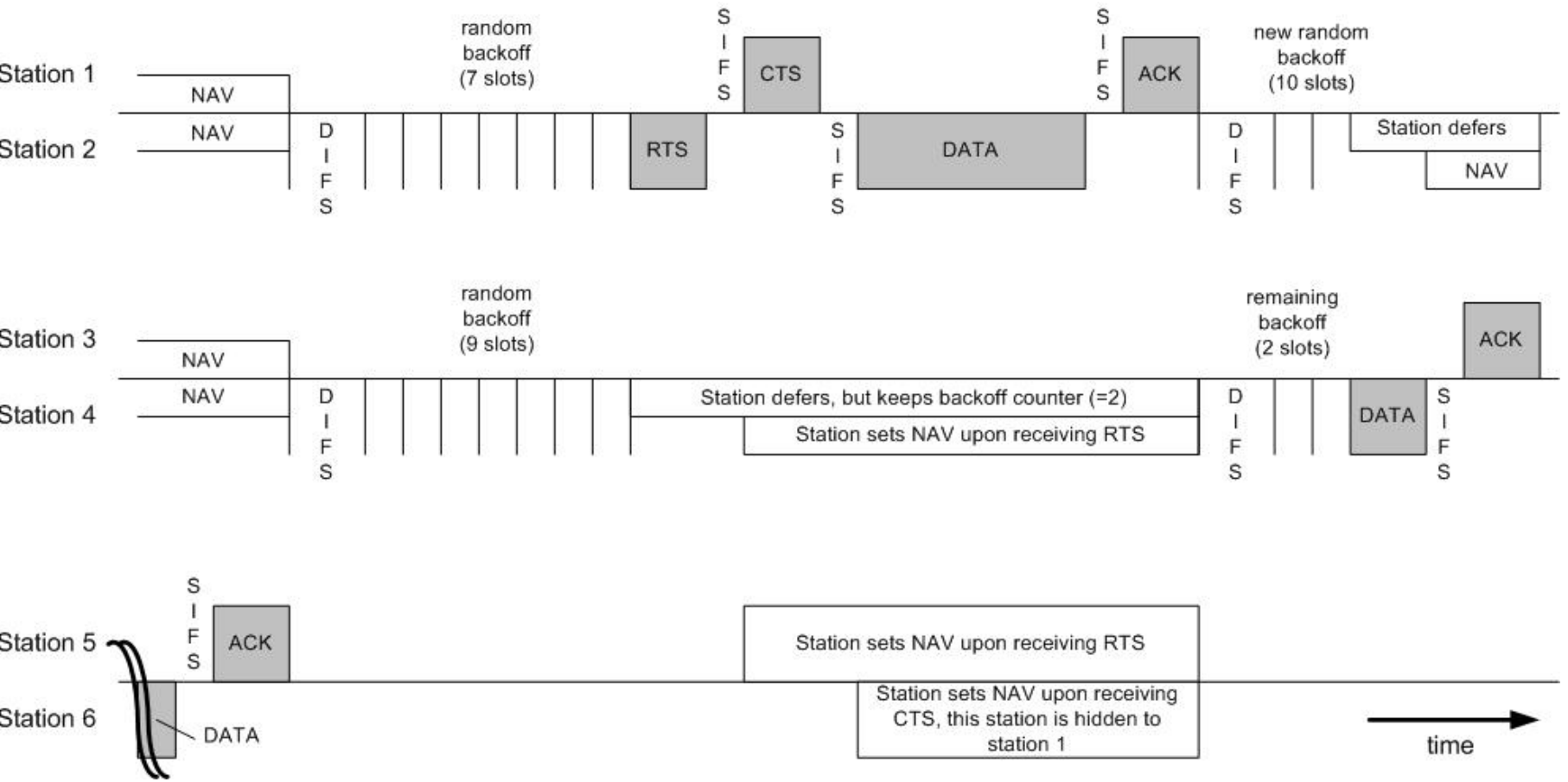
Echange des données en utilisant : RTS-CTS



Echange : RTS-CTS

- 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
  - De ne l'utiliser que lorsque la trame à envoyer excède une variable RTS_Threshold
  - De ne jamais l'utiliser

DCF : Résumé


Station 1
Station 2
Station 3
Station 4
Station 5
Station 6
NAV
NAV
NAV
NAV
DIFS
random backoff (7 slots)
RTS
SIFS
CTS
SIFS
DATA
SIFS
ACK
DIFS
new random backoff (10 slots)
Station defers
NAV
DIFS
random backoff (9 slots)
Station defers, but keeps backoff counter (=2)
Station sets NAV upon receiving RTS
DIFS
remaining backoff (2 slots)
DATA
SIFS
ACK
SIFS
ACK
DATA
Station sets NAV upon receiving RTS
Station sets NAV upon receiving CTS, this station is hidden to station 1
time

PCF

- PCF permet le transfert de données isochrones
- Mise en place : pendant la période CFP (Contention Free Period)
- Fonctionne en alternance avec DCF

- Méthode d'accès basée sur le polling
  - Polling : élimination de contentions
  - Point Coordinator (PC) : au niveau de l'AP
    - Polling Liste
    - PIFS

- Inconvénient : Méthode jamais implémentée au niveau des points d'accès

Fonctionnement de PCF

PC (Point Coordinator)

- si le support est libre au début de la période SCF
  pendant **PISF** sec.

  alors transmission d'une trame Beacon contenant CFPMaxDuration (longueur de la période PCF)

Les stations

- si réception de Beacon

  alors mise à jour du NAV avec CFPMaxDuration

  (Ne transmettent pas pendant CFP)

Fonctionnement de PCF

- Après SIFS interval, le PC peut transmettre les trame de données aux stations

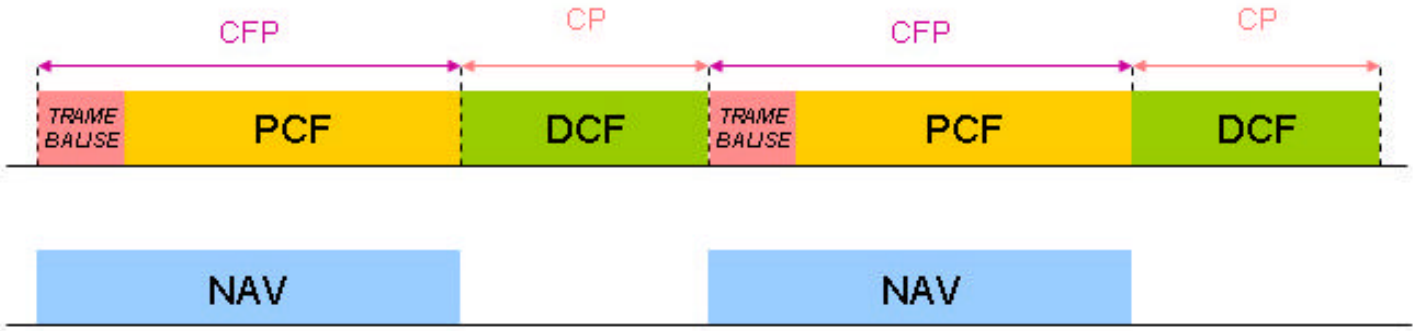
  Trame données (PC → station)
  - unicast, broadcast, multicast
  - La transmission immédiate après PIFS est possible

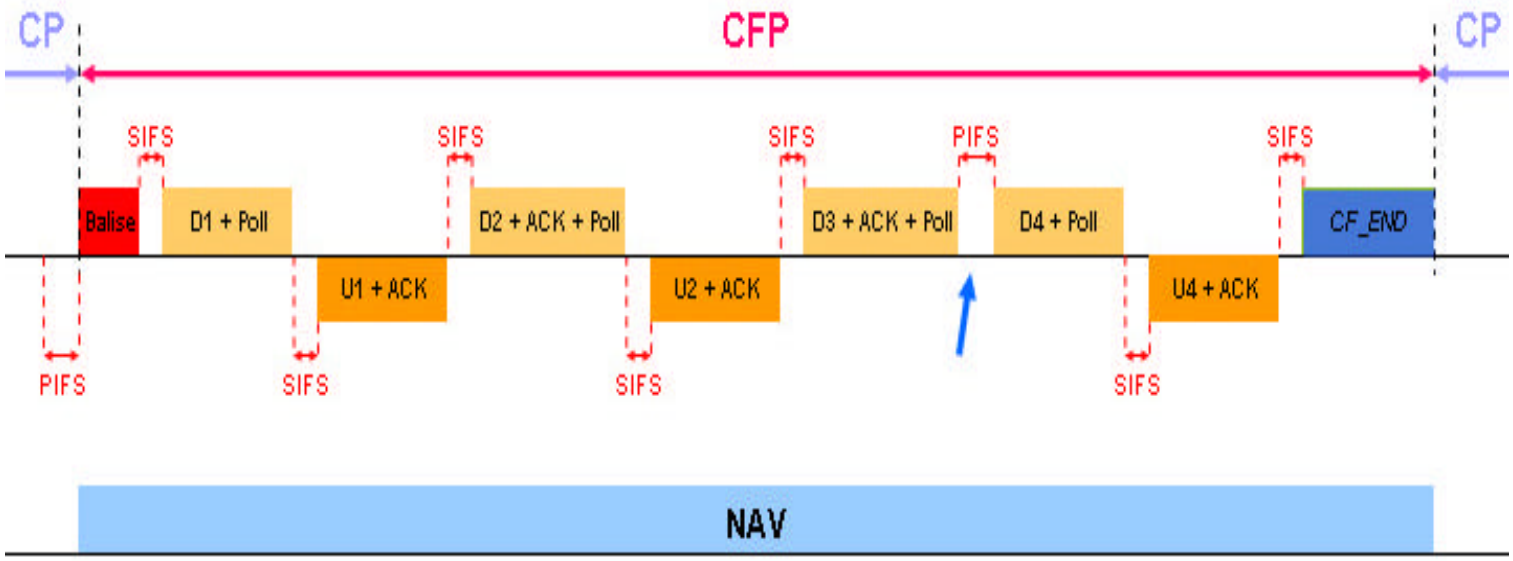
  Trame CF Poll
  - Autorise les stations à transmettre
  - Toutes les destinations sont possibles
  - Transmission d'une seule trame à la foisl

  Trame données + CF Poll (piggyback)

  Trame CF End
  - Annonce la fin de la période CFP

PCF


CFP
CP
CFP
CP
TRAME BALISE
PCF
DCF
TRAME BALISE
PCF
DCF
NAV
NAV


CP
CFP
CP
SIFS
SIFS
SIFS
PIFS
SIFS
Balise
D1 + Poll
D2 + ACK + Poll
D3 + ACK + Poll
D4 + Poll
CF_END
U1 + ACK
U2 + ACK
U4 + ACK
PIFS
SIFS
SIFS
SIFS
NAV

Couche liaison : autres fonctions

- Accès au réseau
- authentification et sécurité
- Fragmentation – réassemblage
- Handover
- Économie d'énergie
- Trames 802.11

Initialisation/Accès au réseau

- Allumer station → phase de découverte
  - Découvrir l'AP et/ou les autres stations
- Présence détectée → rejoindre le réseau
  - Service Set Id (SSID) : nom du réseau de connexion
  - Synchronisation
  - Récupération des paramètres de PHY
- Négocier la connexion
  - Authentication & Association

Phase de découverte du réseaux

- Phase d'écoute
  - • écoute passive / écoute active
- Écoute passive
  - La station attend de recevoir une trame balise (Beacon)
  - A la réception de Beacon prendre les paramètres (SSID & autres)
- Écoute active
  - La station envoie directement une requête d'association (Probe Request Frame)
  - Attendre la réponse de l'AP ou des autres stations

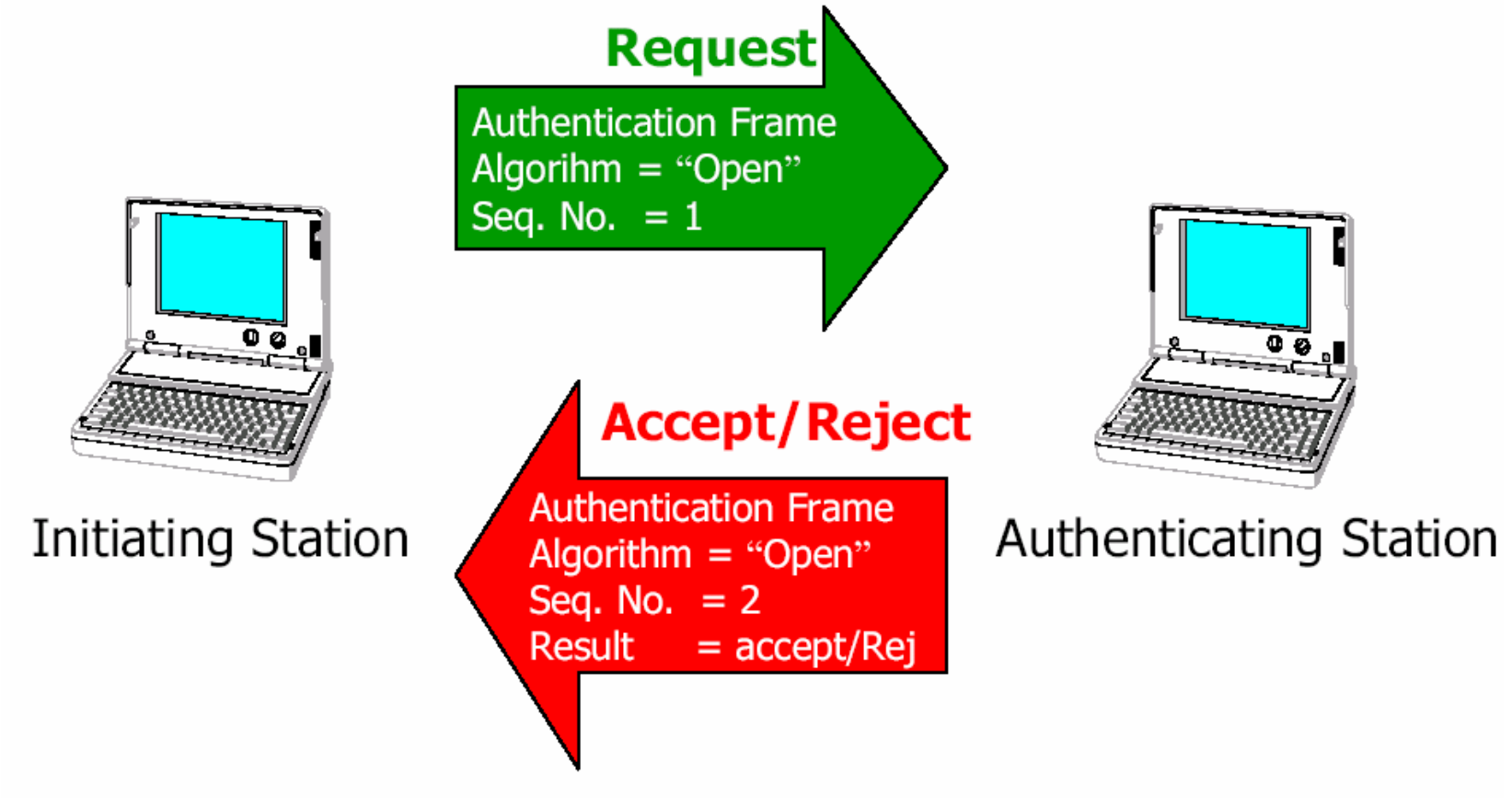
Authentication

- Se protéger contre les accès non autorisés

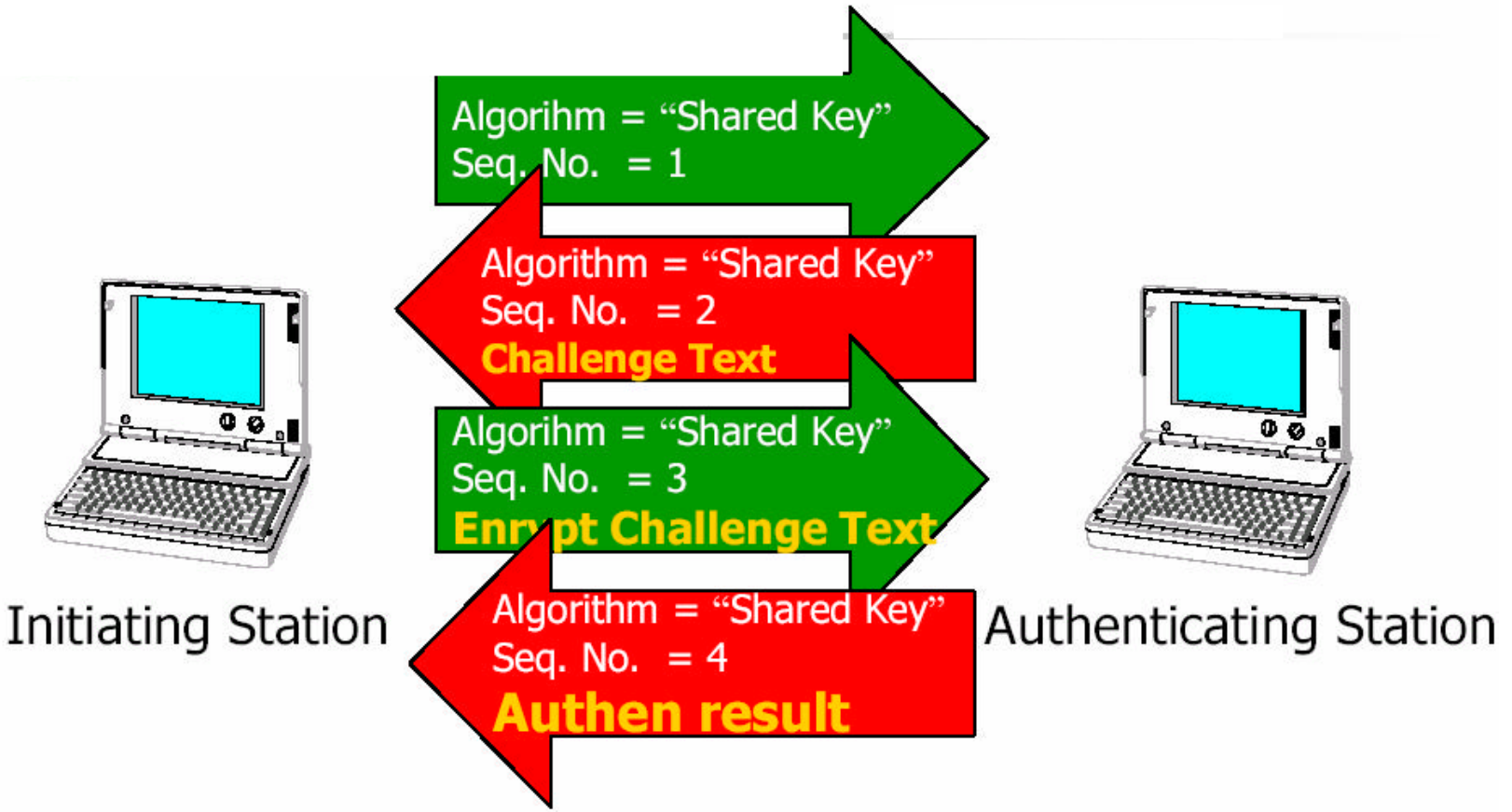
- Open system authentication
  - Mode par défaut

- Shared key authentication
  - Plus haut degré de sécurité
  - Echange de trame plus rigoureux
  - Utilise le mécanisme WEP (Wired Equivalent Privacy)

Open System Authentification



Shared Key


Algorihm = "Shared Key"
Seq. No. = 1
Algorithm = "Shared Key"
Seq. No. = 2
Challenge Text
Algorihm = "Shared Key"
Seq. No. = 3
Encrypt Challenge Text
Algorithm = "Shared Key"
Seq. No. = 4
Authen result
Initiating Station
Authenticating Station

Failles dans 802.11

- Tous les mécanismes de sécurité peuvent être déjoués
- Solutions :
  - A court terme
    - WEP +
    - 802.1x avec EAP (Extended Authentication Protocol)
  - A long terme
    - 802.11i basé sur AES (Advanced Encryption Standard)

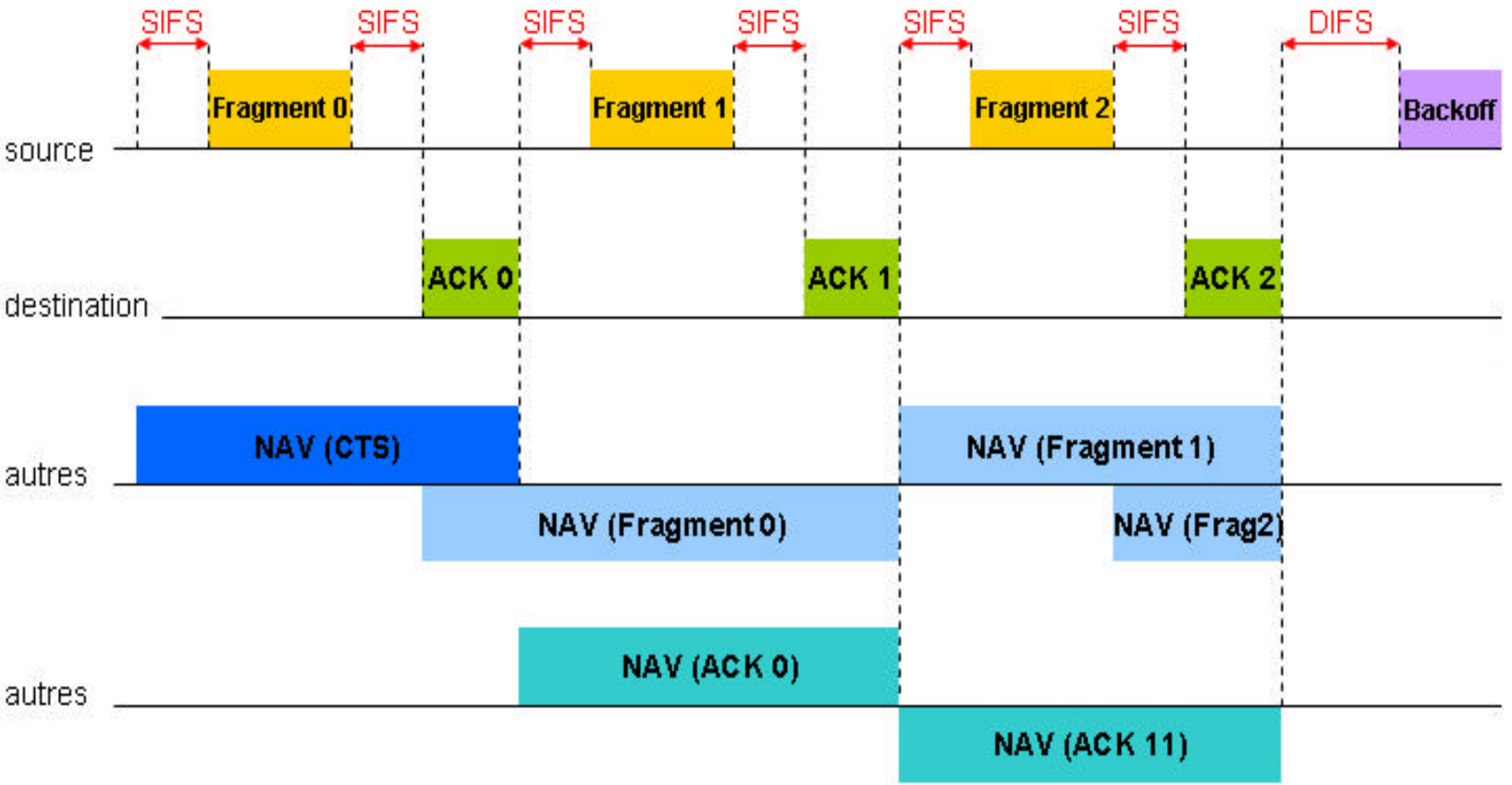
Fragmentation - réassemblage

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

Fragmentation - réassemblage

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

Fragmentation - réassemblage



Handover

- passage d'une cellule à une autre sans interruption de la communication
  - Le standard ne définit pas de handover de roaming dans les réseaux 802.11
  - 802.11f en cours de développement
- Le standard définit quelques règles à respecter
  - Synchronisation
  - Écoute active et passive
  - Mécanismes d'association et de réassociation, qui permettent aux stations de choisir l'AP auquel elles veulent s'associer
- Sécurité renforcée pour éviter :
  - qu'un client ne prenne la place d'un autre
  - Qu'il n'écoute les communications d'autres utilisateurs

Économie d'énergie

- Problème principal des terminaux mobiles: faible autonomie de la batterie
  - Mode d'économie d'énergie prévu par le standard

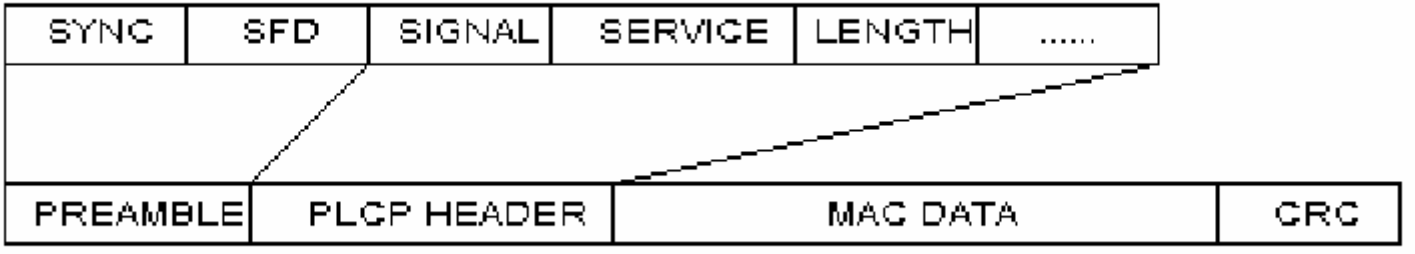
- 2 modes de travail pour le terminal
  - Continuous Aware Mode
    - Fonctionnement par défaut
    - La station est tout le temps allumée et écoute constamment le support
  - Power Save Polling Mode

Power Save Polling

- Permet une économie d'énergie
- Géré par le point d'accès
  - L'AP tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie
  - Stocke toutes les données qui leur sont adressées
  - Les stations en veille s'activent périodiquement pour recevoir une trame TIM (Traffic Information Map), envoyée par l'AP
    - Si l'AP possède des données destinées à la station, celle-ci envoie une requête à l'AP : Polling Request Frame
- Entre les trames TIM, les terminaux retournent en mode veille

Structure des trames

- Préambule : dépend de la couche physique
  - Séquence Synch pour sélectionner l'antenne à laquelle se raccorder
  - Séquence SFD (Start Frame Delimiter) pour définir le début de la trame
- PLCP : infos logiques utilisées par la couche physique pour décoder la trame
- Données MAC
- CRC



Structure des trames

PDU FHSS

Préambule		En-tête			MPDU
Synch 80 bits	*SFD* 16 bits	*Length* 12 bits	*PSF* 4 bits	*CRC* 16 bits	

réambule

ynch : c'est une séquence de 80 bits alternant 0 et 1, qui est utilisée pour sélectionner AP appropriée (détermine du gain radio) ainsi que pour la synchronisation.

FD : Le Start Frame Delimiter consiste en une suite de 16 bits (0000110010111101) ui définit le début de la trame.

n-tête :

ength : il représente le nombre d'octets que contient le paquet, ce qui permet à la ouche physique de détecter correctement la fin de la trame.

SF : Le Payload Signaling Field contient l'information sur le débit utilisé ainsi que uelques bits qui pourront être utilisé pour un usage futur.

RC : champ de détection d'erreur

Structure des trames

PDU DSSS

Préambule		En-tête				MPDU
Synch 128 bits	*SFD* 16 bits	*Signal* 8 bits	*Service* 8 bits	*Length* 16 bits	*CRC* 16 bits	

Préambule

Synch : c'est une séquence de 128 bits qui est utilisé pour la détection du signal.

SFD : ce champ indique le début de la trame.

En-tête

Signal : ce champ indique le débit utilisé.

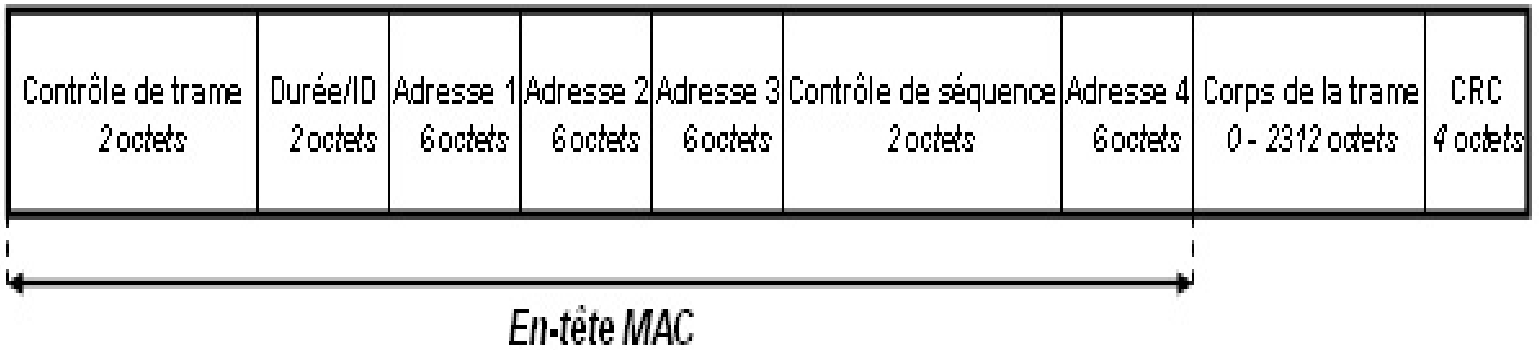
Service : ce champ est réservé pour un usage futur, il ne contient que des 0 pour le moment

Length : il représente le nombre d'octets que contient la trame.

CRC : champ de détection d'erreur.

Structure des trames MAC

MPDU



Structure des trames MAC

rame de contrôle

Version de protocole	Type	Sous type	To DS	From DS	More frag	Retry	Pwr mgt	More data	WEP	Order
2 bits	*2 bits*	*4 bits*	*1 bit*	*1 bit*	*1 bit*	*1 bit*	*1 bit*	*1 bit*	*1 bit*	*1 bit*

ersion de protocole : ce champ contient 2 bits qui pourront être utilisés pour reconnaître des versions utures possibles du standard 802.11. Dans la version courante, la valeur est fixée à 0.

ype et sous-type : les 6 bits définissent le type et le sous-type des trames.

o DS : ce bit est mis à 1 lorsque la trame est adressée à l'AP pour qu'il la transmette au DS. Ceci inclut le as où le destinataire est dans la même cellule et que l'AP doit relayer la trame. Le bit est à 0 dans toutes s autres trames.

rom DS : ce bit est mis à 1 lorsque la trame vient du DS.

ore Fragments : ce bit est mis à 1 lorsque d'autres fragments suivent le fragment en cours.

etry : ce bit indique que la transmission du fragment (ou d'une trame) en cours est une retransmission un fragment(ou d'une trame) précédemment transmis. Ainsi la station destination peut reconnaître les oublons ce qui peut arriver lorsqu'un ACK se perd.

ower Management : ce bit est utilisé pour la gestion de l'énergie. Il indique à la station quelle passera en ode d'économie d'énergie juste après la fin de la transmission de cette trame. Grâce à ce bit, les stations euvent changer de mode de fonctionnement passant ainsi du mode veille au mode actif ou inversement.

ore Data : ce bit est aussi utilisé pour la gestion de l'énergie. Il utilisé par l'AP pour indiquer que des ames sont stockés pour une station. La station peut demander à recevoir les autres trames ou peut grâce cette information passer en mode actif.

EP : ce bit indique que le corps de la trame est chiffré avec l'algorithme WEP.

rder : 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 e changement d'ordre entre les trames unicast et multicast.

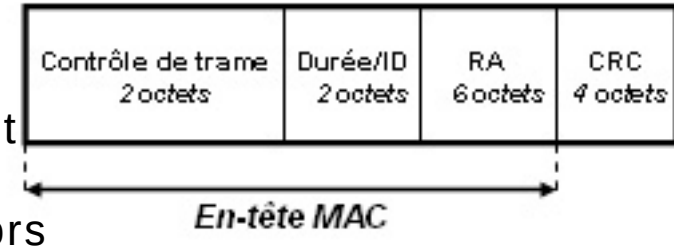
Structure des trames(RTS, CTS, ACK)

rame RTS

A : correspond à l'adresse de la station destination.
A : correspond à l'adresse de la station source qui émet la trame RTS.
e champ durée de vie correspond au temps qui est nécessaire pour la transmission de la rame RTS auquel on ajoute le temps de transmission d'une trame CTS et le temps de ransmission d'une trame ACK ainsi que trois SIFS.

rame CTS

A : correspond à l'adresse de la station source qui rovient du champ TA de la trame RTS.
e champ durée de vie correspond a la valeur du champs durée de vie ans la trame RTS moins le temps de transmission de la trame CTS et d'un SIFS



rame ACK

A : correspond à l'adresse de la station source qui provient u champ adresse 2 de la trame précédente.
i le bit More Fragment de la trame précédente est à 0 alors e champ durée de vie a pour valeur 0. Sinon il correspond au champ durée le vie de la trame précédente moins le temps de transmission de la trame ACK et un SIFS.