Réseaux mobiles

Isis TRUCK

Bibliographie

- 802.11 Réseaux sans fil – La référence, Matthew Gast, *O'Reilly*, 2005
- …

Plan

- Avant propos : généralités réseaux sans fil
- Qu’est-ce que le 802.11?
- Quelques rappels sur réseaux filaires
- Couche MAC du 802.11
- Sécurité
- Couche physique (PHY)
- Travaux pratiques

Avant propos (1/3)

- Réseaux sans fil:
  - mobilité (dans la limite de la portée de la station de base ou *point d'accès*)
  - Souplesse (facilité et rapidité de déploiement)
    - Pas besoin de passer de câbles (long, cher, pénible)
    - Besoin de points d'accès et d'antennes et d'une simple autorisation pour connecter un nouveau venu)
    - Cf. par exemple les zones d'accès sans fil publiques (*hotspots*)
  - Transmission des données *via* des radiations électromagnétiques – ondes radio
  - NB : une onde radio est une onde électromagnétique. Une onde électromagnétique permet de décrire une radiation électromagnétique. Un rayonnement électromagnétique a comme vecteur le photon (particule dépourvue de masse). Une onde électromagn. correspond à la propagation d'un champ magnétique. On la détecte via la variation des champs magnétique et électrique.

Avant propos (2/3)

- fréquence d'une onde radio est inférieure à 3 000 GHz, soit une longueur d'onde supérieure à 0,1 mm
- Le Wifi utilise des ondes UHF (*ultra high frequency*) dont la fréquence va de 300 MHz à 3 GHz et la longueur d'onde de 1 m à 10 cm (ondes décimétriques GSM, GPS, Wi-Fi)
- Rappels sur fréquence. F = 1/T, T étant la période en secondes et T en Hertz)
- Ondes sont émises dans une certaine bande de fréquence
- Chaque bande a une certaine ***largeur (de bande)*** :
  - Si bcp d'infos (càd signaux complexes) alors nécessité d'une large bande (ex. signaux TV : 6 MHz)

Avant propos (3/3)

– Bandes de fréquences allouées (France)

ISM : Industriel, Scientifique et Médical.
Ex. four micro-ondes
=> 2,4 GHz

Bande	**Intervalle de fréquence**
GSM	890 – 915 MHz
DECT	1880 – 1900 MHz
Bande S ISM (802.11 b/g)	2,4 – 2,5 GHz
Bande C	4 – 8 GHz
Bande C, lien satellite descendant	3,7 – 4,2 GHz
Bande C ISM (802.11a)	5,725 – 5,875 GHz
Bande C, lien satellite montant	5,925 – 6,425 GHz
Bande X (militaire)	8 – 10 GHz
Bande Ku (TV par satellite)	10 – 12 GHz

Qu’est-ce que le 802.11?
(ou Ethernet vs. 802.11)

• Globalement, 802.11 # (peu différent) Ethernet, càd 802.11 adapte les techno Ethernet classiques au monde du sans fil. 802.11 correspond aux couches 1 et 2 du modèle OSI (physique + Liaison de données)

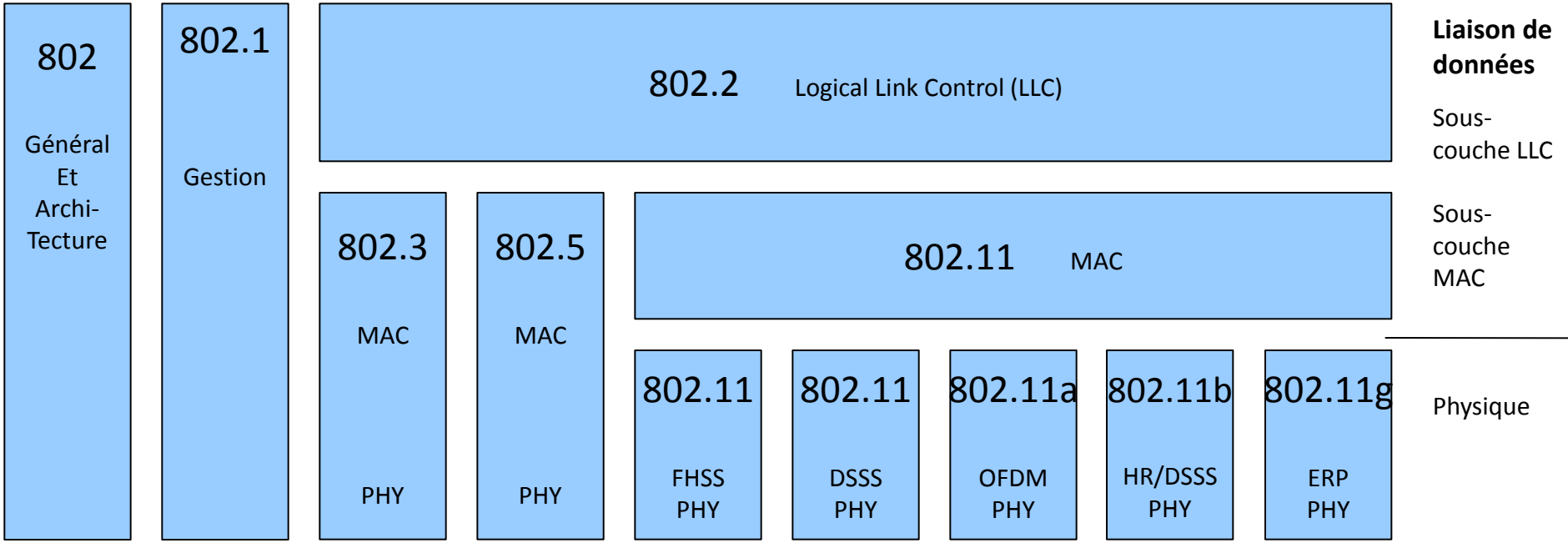
• Cf. aussi Rappels sur Ethernet (après ce sous chapitre)

• La norme 802.11 définit les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- couche physique (notée parfois couche PHY) qui fixe les détails pour l'émission et la réception des données. Elle propose 3 types de codage de l'information,
- couche liaison de données qui établit règles définissant la façon d'accéder au support et d'envoyer les données. Elle est constituée de 2 sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au medium (Media Access Control, ou MAC)

Schéma général

Famille IEEE 802 est constituée d'un ensemble de spécifications pour les technologies de réseaux locaux (LAN) :



Couches du 802.11 (1/4)

802.3 : CSMA/CD

802.5 : Token Ring

Spécification 802.11 de base = 801.11 MAC + 2 couches physiques (1 couche physique par étalement spectre par saut de fréq. FHSS (Frequency-hopping Spread-spectrum) + 1 couche liaison par étalement spectre à séquence directe DSSS (Direct-sequence Spread-spectrum))

802.11a : spécification d'une couche avec division orthogonale de fréquence (OFDM – Orthogonal Frequency Division Multiplexing)

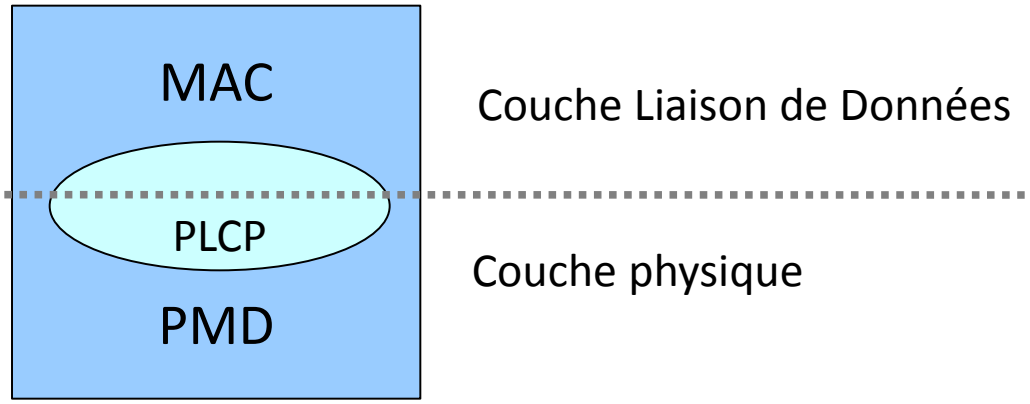
802.11b : spécification d'une couche à séquence directe à haut débit (HR/DSSS)

802.11g : couche de physique la + récente. Offre vitesses + élevées grâce à OFDM, mais rétro-compatibilité aussi avec 802.11b

NB : Attribution d'une @ MAC se fait à partir de la même réserve d'adresses et les cartes 802.11 ont donc des adresses uniques, même lorsqu'elles sont dans un réseau Ethernet filaire.

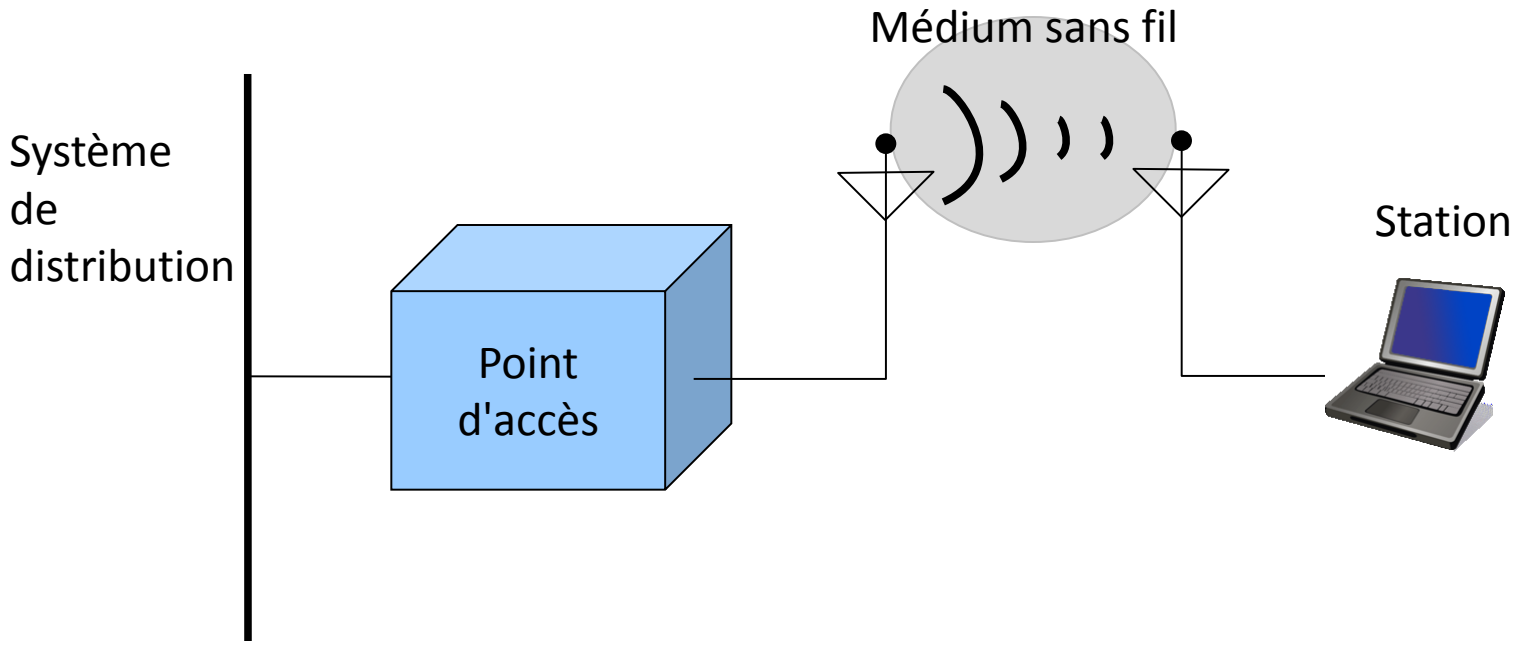
Couches du 802.11 (2/4)

- L'utilisation des ondes radio comme support physique implique une PHY complexe, séparée en 2 composants :
  - PLCP: procédure de convergence de la couche physique (Physical Link Convergence Procedure)
  - PMD: système dépendant du medium physique pour transmettre trames (Physical Medium Dependent)
- PLCP sert d'interface entre MAC et couche physique



Couches du 802.11 (3/4)

- 4 composants physiques principaux illustrent les réseaux 802.11 :



Couches du 802.11 (4/4)

- 4 composants physiques principaux illustrent les réseaux 802.11 :
  - *Station* : un réseau est fait pour transférer des données entre *stations*. Les stations sont des périphériques dotés d'interface réseau sans fil (carte réseau). D'ordinaire, les stations sont des ordinateurs (portables ou non). Mais toutes sortes d'appareil peuvent être des stations (chaîne stéréo, TV, caméra, …)
  - *Point d'accès (access point* ou *AP)*: servent à convertir les trames 802.11 en trames du monde filaire. Sert de pont entre le sans fil et le filaire.
  - *Médium sans fil* : il s'agit de la couche physique. En fait, plusieurs couches physiques ont été normalisées (par fréquences radio mais aussi par infrarouges)
  - *Système de distribution* noté **DS** pour *Distribution System* :
    - L'idée du sans fil est (aussi) d'offrir une grande zone de couverture en permettant la mobilité des *stations*.
    - Une même *station* peut donc se connecter successivement à plusieurs *points d'accès* (en se déplaçant).
    - Le *système de distribution* sert donc à suivre ces déplacements, càd qu'il est le composant logique du 802.11 permettant de renvoyer les trames vers leur destination.
    - On l'appelle le ***réseau dorsal***. Ds bcp de cas, c'est Ethernet qui sert de réseau dorsal.
    - *DS* peut être aussi bien un réseau filaire, qu'un câble entre deux points d'accès ou bien même un réseau sans fil !

Types de réseaux (1/7)

• Elt de base d'un réseau 802.11 est constitué d'un BSS (*Base Service Set* : ens. des services de base), càd un groupe de stations qui communiquent.

• Qd une station se trouve ds *l'aire de service de base* (= zone où la communication sans fil « passe »), elle peut communiquer avec les autres membres du BSS.

• Chaque *BSS* est identifié par un *BSSID* (6 octets).

• On distingue 2 variantes pour le BSS

- **BSS indépendant (IBSS)** : stations seules, sans point d'accès
- **BSS infrastructure** : stations avec point d'accès.

•IBSS :

- •Constitué au minimum de 2 stations
- •stations se connectent les unes aux autres afin de constituer un réseau point à point (*peer to peer*), c-à-d un réseau dans lequel chaque machine joue 2 rôles à la fois : celui de client et celui de point d'accès.

Types de réseaux (2/7)

- IBSS (suite)
  - Solution couramment employée pour créer un réseau à courte durée de vie ds le cadre d'une conférence, par ex. => *réseau éphémère* encore appelé BSS *ad hoc* ou *réseau ad hoc*.
  - Comme le BSS infrastructure, il est identifié par un *SSID*
  - NB : un IBSS est dit « réseau sans fil restreint »:
    - portée du *IBSS* est déterminée par la portée de chaque station
    - Les stations ne peuvent communiquer que 2 à 2 (pas de transitivité)
    - Càd que si 2 des stations du réseau sont hors de portée l'une de l'autre, elles ne pourront pas se parler, même si elles « voient » d'autres stations car, contrairement au mode infrastructure, le mode *ad hoc* ne propose pas de *système de distribution* capable de transmettre les trames d'une station à une autre.

Types de réseaux (3/7)

- BSS infrastructure
  - Présence de points d'accès (passage obligatoire)
  - Communication se fait en 2 étapes :
    - Station émettrice envoie la trame au point d'accès
    - Le point d'accès la transfère à son destinataire
  - Ce mode « centralisé » a bcp d'avantages (à commencer par l'économie d'énergie au niveau des stations)
  - Ds un BSS infrastructure, les stations doivent être *associées* à un point d'accès afin de bénéficier des services réseau. Cette *association* correspond à l'équivalent logique du branchement du câble réseau à la prise Ethernet.
  - Ce sont les stations qui initient cette demande d'association et les points d'accès peuvent accepter ou refuser.
  - Les associations sont exclusives : une station ne peut être reliée qu'à un et un seul point d'accès

Types de réseaux (4/7)

- BSS infrastructure (suite)
  - Dans ce mode *infrastructure*, le *BSSID* correspond en fait à l'adresse MAC du point d'accès
- Aires de services étendues
  - Les BSS ne permettent que de couvrir des petits bureaux et des domiciles.
  - Mais 802.11 autorise la création de réseaux sans fil de taille quelconque en reliant des BSS au sein d'un *ensemble de services étendu* (*extended service set* ou ***ESS***).
  - Un ESS est donc créé en chaînant des BSS et un réseau dorsal (ou DS).
  - Tous les points d'accès d'un ESS reçoivent le même identifiant d'ensemble de services (***SSID*** – *service set identifier*) qui sert de nom de réseau pour les utilisateurs (32 caractères de long, soit 32 octets)

Types de réseaux (5/7)

- Changement de BSS dans un ESS
  - Lorsqu'un utilisateur nomade passe d'un *BSS* à un autre lors de son déplacement au sein de l'*ESS*, sa station est capable de changer de point d'accès selon la qualité de réception des signaux (des dits points d'accès).
  - Les points d'accès communiquent entre eux grâce au système de distribution afin d'échanger des informations sur les stations et permettre le cas échéant de transmettre les données des stations mobiles.
  - Cette caractéristique permettant aux stations de « passer de façon transparente » d'un point d'accès à un autre est appelé *itinérance* (**roaming**).

Types de réseaux (6/7)

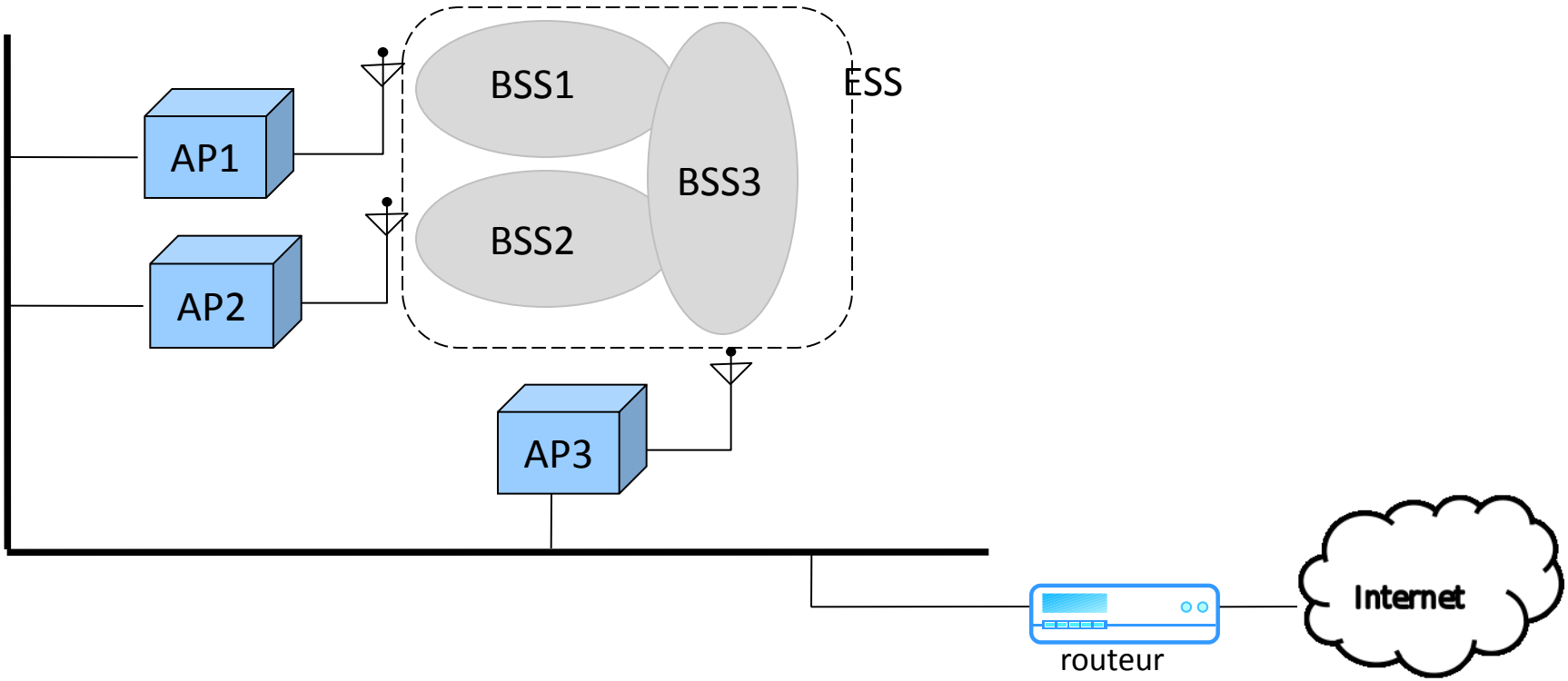
- Communication entre 2 stations d'un même ESS mais dans des BSS différents
  - Les points d'accès jouent donc le rôle de ponts et
  - Le réseau dorsal (DS) doit ressembler à une connexion de la couche 2 (technologie de tunnel pour simuler un environnement de couche 2)
  - Càd que les points d'accès d'un ESS fonctionnent de concert afin que le monde extérieur puissent communiquer avec une station quelconque au sein de l'ESS via son adresse MAC.
- Le système de distribution
  - On l'a vu, le DS fournit la mobilité en connectant les points d'accès
  - Qd une trame est passée au DS, elle est envoyée au point d'accès adéquat, qui la redirige vers la bonne station (le destinataire)

Types de réseaux (7/7)

• DS est responsable du suivi de l'emplacement physique d'une station et de la livraison adéquate des trames.

• Dans le schéma suivant, le routeur ne connait que l'adresse MAC de la station mobile (destinataire). C'est le DS qui doit trouver l'AP adéquat.

• Naturellement, chaque AP connaît les stations qui lui sont associées AINSI QUE la liste des stations qui sont associées aux AP avec lesquels il communique.



Services réseau (1/4)

- Le 802.11 fournit 9 services (càd que cela donne une indication aux fournisseurs de matériels qui veulent vendre du matériel Wifi : ils peuvent implémenter ces 9 services comme ils le souhaitent)
  - 3 pour la transmission des données
  - 6 pour la gestion pour le suivi des nœuds mobiles et la livraison des trame sans erreur
- Les 9 services
  - *Distribution* : service utilisé par les stations dans un IBSS chaque fois qu'elles envoient une donnée (à « leur » AP). C'est l'AP qui utilise à son tour ce service pour transmettre la trame au destinataire
  - *Intégration* : service fourni par le système de distribution. Il permet la connexion du sys de distr à un réseau non-IEEE 802.11. Cette fonction est spécifique au réseau « étranger » en question, donc n'est pas spécifiée dans 802.11, exceptée en termes de services qu'elle doit offrir.
  - *Association* : Les stations s'associent aux AP. Ds le cas de protocoles de sécurité élevée, le trafic réseau ne pourra se faire qu'UNE FOIS l'authentification réussie.
  - *Réassociation* : lors du « nomadisme » des stations (lorsqu'elle passe d'un BSS à un autre). La station doit évaluer la force du signal des BSS et choisir le meilleur (décider si elle doit changer ou non).

Services réseau (2/4)

• *Dissociation* : Pour clore une association existante. Forme de « politesse » pendant l'arrêt de la station. Cela dit, MAC est conçu de manière à pouvoir se passer de la dissociation et prendre en charge les stations qui quitteraient le réseau sans *dissociation*.

• *Authentification* : indispensables pour vérifier que les utilisateurs sont bien autorisés à se connecter. Problème criant en mode sans fil (!) . Authentification peut se produire à plusieurs moments : avant l'association (vérification d'identité minimale avec l'adresse MAC), et bien sûr lorsque l'utilisateur s'authentifie (chiffrement robuste, on en reparlera).

• *Désauthentification* : Pour clore une authentification existante. A pour effet secondaire de terminer toute association en cours.

• *Confidentialité* : ds version initiale du 802.11, le service de confidentialité était assuré par le protocole WEP (Wired Equivalent Privacy). Depuis, on a utilisé le WEP 128 bits, WPA, WPA2… (cf. plus loin)

• *Livraison MSDU* (MAC Service Data Unit) : responsable d'envoyer les données à la station finale

Services réseau (3/4)

- *Services supplémentaires définis en 2003 par la norme 802.11h :*
  - Contrôle de la puissance d'émission (TPC : Transmit Power Control) Permet de contrôler la puissance en cohérence avec la règlementation locale ; éviter les interférences avec les réseaux voisins
  - Sélection dynamique de la fréquence (DFS – Dynamic Frequency Selection). Reconfiguration des canaux pour éviter d'interférer avec les radars dans la bande des 5 GHz, au cas où des radars (qui utilisent cette bande) seraient à portée.
- Nota Bene sur l'association (ou la réassociation):
  - Chaque AP diffuse régulièrement (toutes les 0.1 seconde) une **trame balise** (***beacon***) donnant des informations sur son *BSSID*, et éventuellement son *SSID*. Le *SSID* est automatiquement diffusé par défaut, mais il est préférable de désactiver cette option.
  - Lors de l'entrée d'une station dans un ESS, celle-ci diffuse une requête de sondage (*probe request*) contenant le *SSID* pour lequel elle est configurée ainsi que les débits que son adaptateur sans fil supporte. Si aucun *SSID* n'est configuré, la station écoute le réseau à la recherche d'un *SSID*.

Services réseau (4/4)

- Nota Bene sur l'association (suite):
  - A chaque requête de sondage reçue, le point d'accès vérifie le *SSID* et la demande de débit présents dans la *trame balise*. Si le *SSID* correspond à celui de l'AP, ce dernier envoie une réponse contenant des informations sur sa charge et des données de synchronisation. La station recevant la réponse peut ainsi constater la qualité du signal émis par le point d'accès afin de juger de la distance à laquelle il se situe.
  - Une station se trouvant à la portée de plusieurs points d'accès (possédant bien évidemment le même *SSID*) pourra ainsi **choisir** le point d'accès offrant le meilleur compromis de débit et de charge.
  - Lorsqu'une station se trouve dans le rayon d'action de plusieurs points d'accès, c'est elle qui choisit auquel se connecter !

Qqs rappels sur Réseaux filaires

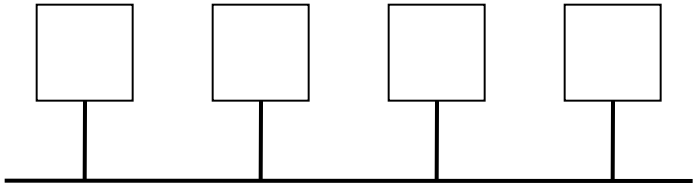
- Topologie
  - Point à Point
  - Multipoint
- Méthodes d'accès au médium (CSMA…)
- Couche Liaison de données
- Protocole de la couche 2
- Sous-couche MAC

Topologie

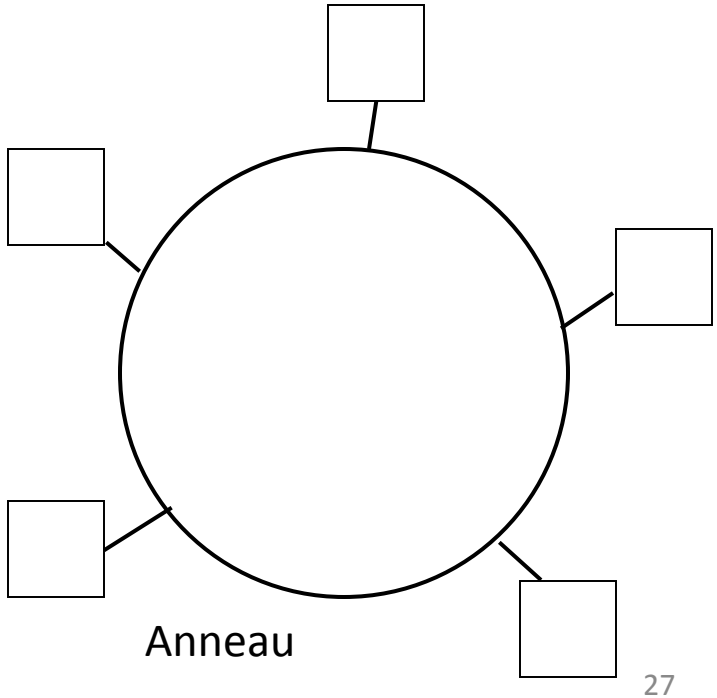
Réseaux en mode diffusion (ou multipoint)

Une seule machine est autorisée à transmettre

➔ nécessite mécanisme d'arbitrage : jeton ; réémission après un temps aléatoire...



Bus



Anneau

Topologie

Réseaux en mode diffusion: *anneau*

Chaque machine qui reçoit un message le recopie vers la machine voisine (circulation en sens unique)

Si le message lui est destiné : conservation

Sinon : destruction

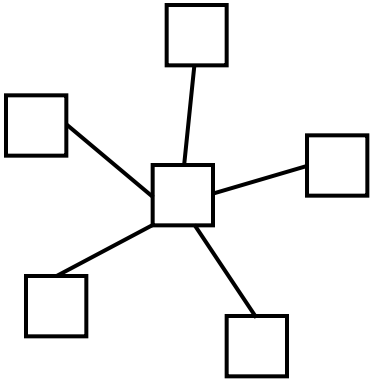
Quand ce mécanisme s'arrête-t-il ?

Y a-t-il moyen de détecter des erreurs ?

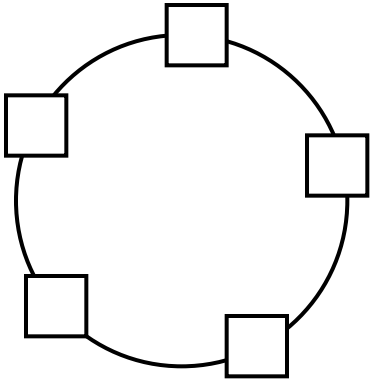
Principal inconvénient d'un anneau?

Topologie

Réseaux en mode point à point

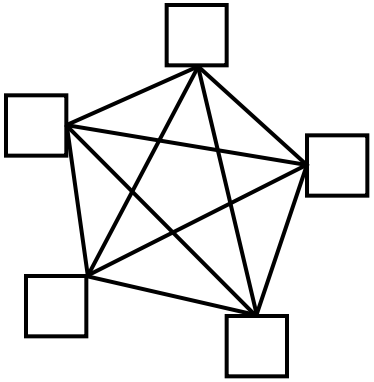


Étoile

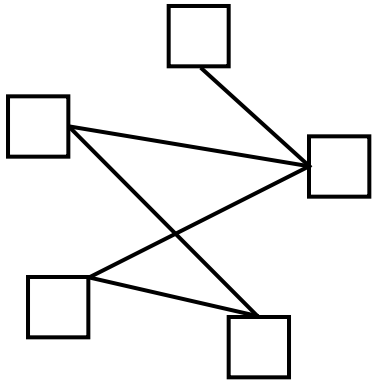


Anneau
(boucle)

Maillage
régulier



Maillage
irrégulier



Topologie

Réseaux en mode point à point

envoi de l'information au destinataire *directement* ou *via des intermédiaires*

cas d'envoi indirect:

données sont reçues puis stockées par l'ordinateur tant que ligne de sortie est occupée

dès que ligne de sortie libre, données sont réexpédiées vers l'intermédiaire suivant

la plupart des WAN utilisent un mode point à point

Méthodes d’accès (mode diffusion)

- comment arbitrer les demandes d’émission des machines sur le medium ?

  2 méthodes principales

  ➔ accès aléatoire

  – ex: Ethernet

  ➔ accès par méthode du jeton

  – ex: anneau à jeton (token ring)

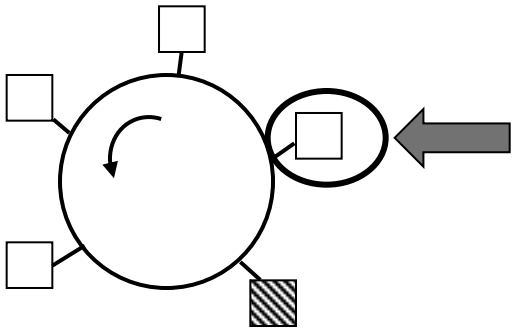
Méthodes d’accès (mode diffusion)

- accès aléatoire
  - selon les protocoles, la machine ***écoute*** ou non avant d’émettre
  - si écoute préalable, attente d’un temps aléatoire si le medium est occupé
  - lorsque 2 ou (plus) machines ont émis en même temps sur le medium, il y a collision, donc destruction de l’information
  - attente d’un temps aléatoire
  - puis réémission de l’information

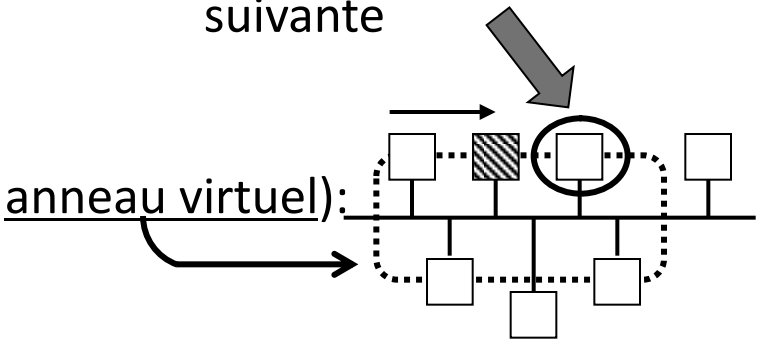
  - *Cf. slides suivants, à partir de la page 62 notamment.*

Méthodes d'accès (mode diffusion)

- accès par méthode du jeton
  - **jeton**: message (trame spéciale) donnant un droit d'accès au medium à la machine qui le détient
  - si machine détenant le jeton n'a rien à émettre, elle le transmet à *la machine suivante*:
    - cas anneau:



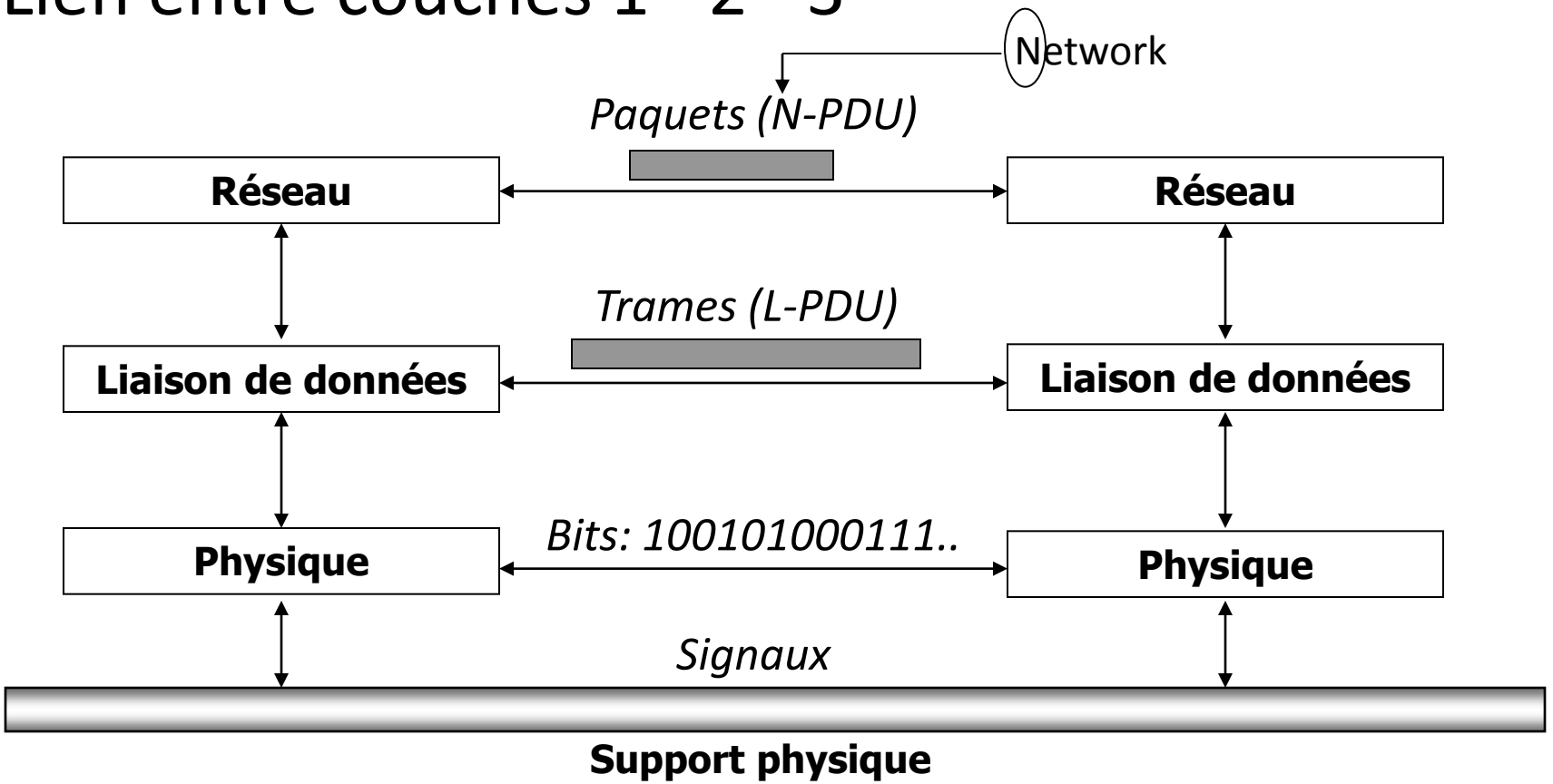
    - cas bus (création d'un anneau virtuel):



  - possibilité de régénérer le jeton s'il a été perdu

Couche liaison de données

- Lien entre couches 1 - 2 - 3



Couche liaison de données (LdD)

- Le protocole de la couche LdD définit
  - Le **format** des messages échangés
  - La **sémantique** des messages échangés
  - Les **règles** d'échange

- Messages échangés appelés **Trames**

Couche liaison de données

- Rôle:
  - Fournir les services nécessaires pour *établir*, *maintenir* et *libérer* une connexion
  - Acheminer les *trames* sur la liaison physique
  - Contrôler le *flux de données* afin d'éviter la saturation du récepteur
  - Contrôler la *correction* de la transmission des données (erreurs venant de la couche physique)

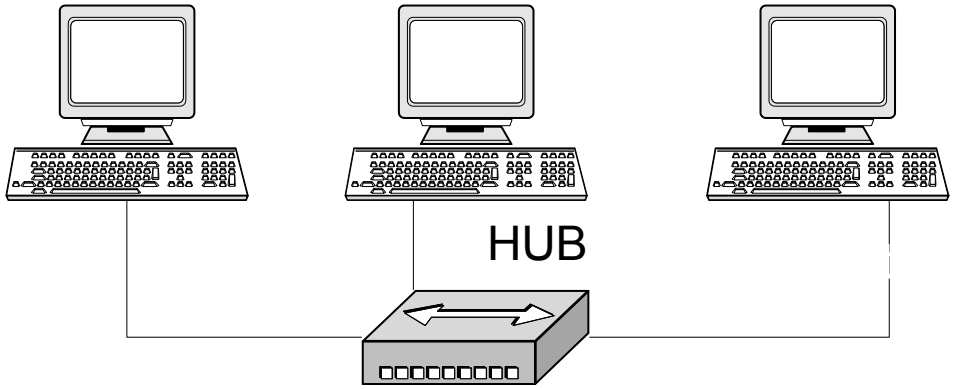
Couche LdD : Rôle

- 2 types de liaison: point à point et par diffusion
  - Les liaisons point à point

ß => Le rôle de la couche liaison se limite aux objectifs précédents.

Couche LdD : Rôle

- Les liaisons par diffusion (canaux partagés).



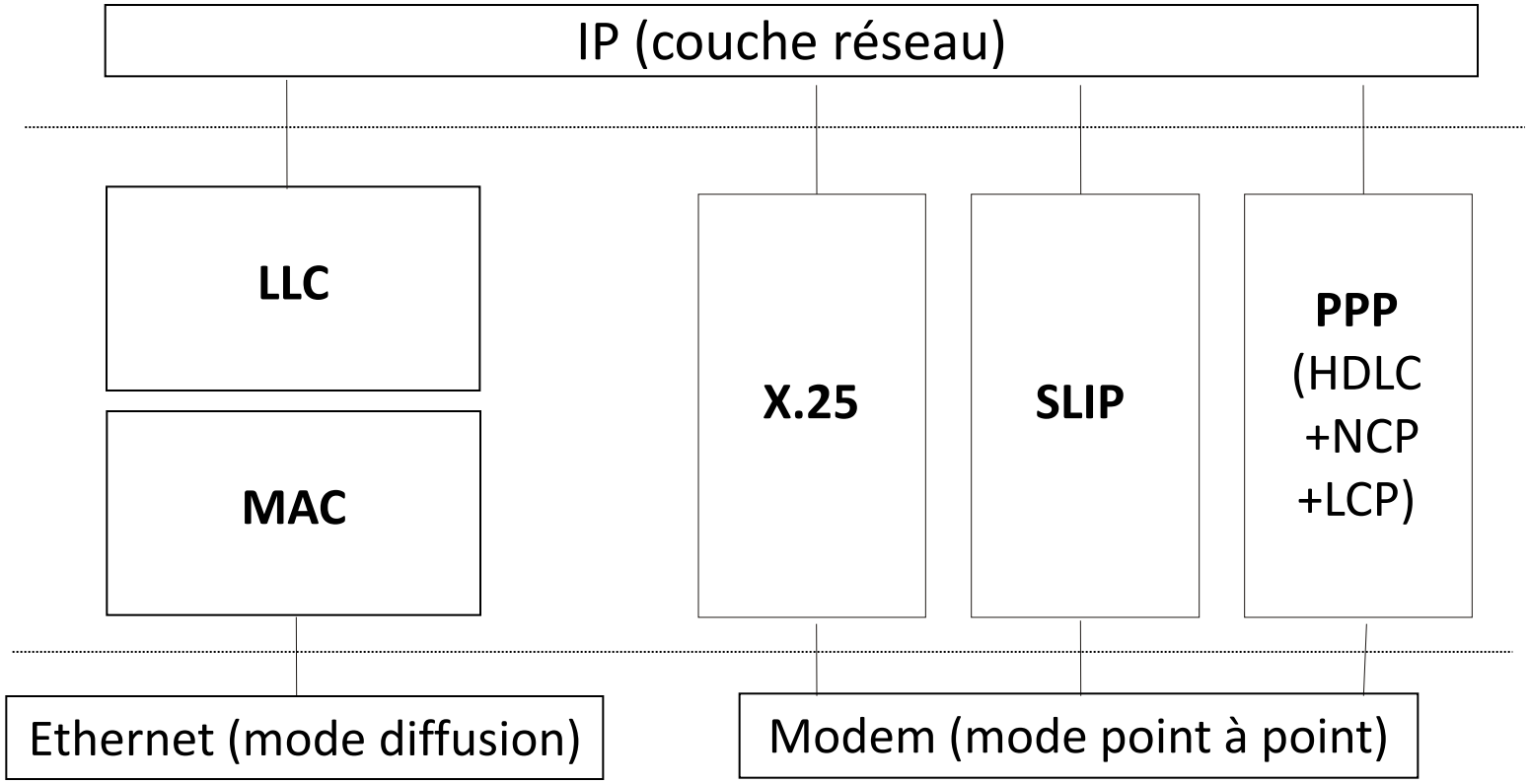
=> En plus des rôles pré-cités, la couche liaison doit gérer le problème de la mise en commun et donc de l'accès au canal de transmission

Couche LdD : Rôle

- Une distinction est souvent faite entre :
  - les fonctionnalités de base de la couche liaison que l'on regroupe en une sous-couche LLC (Logical Link Control)
  - les problèmes spécifiques aux accès des médias partagés que l'on regroupe en une sous-couche MAC (Medium Access Control)

Couche LdD : Rôle

- Quelques organisations possibles de la couche liaison de données



Couche LdD : Services

- Type de services offerts à la couche réseau:
  - sans connexion et sans accusé de réception (sans acquittement)
    - aucune connexion préalable
    - si trame perdue, tant pis
    - convient si:
      - taux d'erreur faible et correction des erreurs prévue ds les couches supérieures
      - ou bien si trafic temps réel
    - exemples d'utilisation:
      - dans les réseaux locaux
      - pour le transport de la parole

Couche LdD : Services

- sans connexion et avec accusé de réception
  - pas de connexion logique
  - toutes les trames sont acquittées
  - utilisé sur des canaux peu fiables (ex: liaisons sans fil)
- connexion avec accusé de réception
  - établissement d'une connexion
  - numérotation de la trame
  - chaque trame est *acquittée*, doit être reçue *une et une seule fois*, et dans l'*ordre* d'émission
  - utilisé pour des transmissions fiables

Couche LdD : Trames

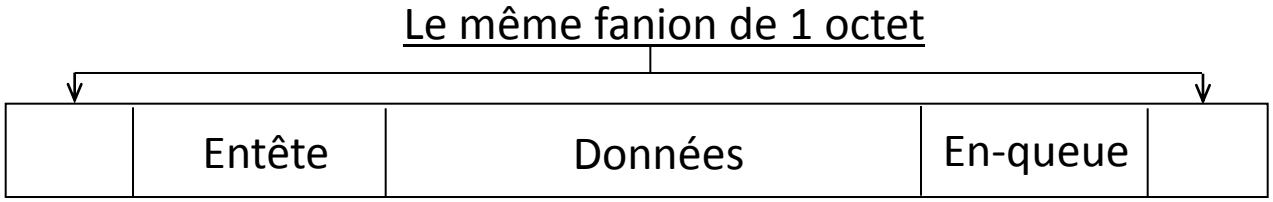
- Messages échangés dans la couche LdD sont appelés **Trames**
  - Trame = L-PDU
  - L-PDU = L-SDU + L-PCI
- Une trame est une suite de bits
- Selon le protocole, elle peut être de taille fixe ou variable (mais bornée). Par ex.,
  - *X25.2, Ethernet : Taille variable*
  - *ATM : Taille fixe (53 octets)*

Couche LdD : Trames

- Structure varie selon le protocole, mais souvent divisée en 3 parties : **entête**, **données** et **terminaison**.
- L'entête et la terminaison forment le L-PCI
- Formation des trames à partir des bits pas toujours simple.
- Pour délimiter les trames, 3 principales solutions :

Couche LdD : Trames

- utilisation de fanions (flags) de signalisation en remplissant des octets



- si, dans les données à transmettre, se trouve justement la configuration binaire du fanion, la couche LdD de l'émetteur *insère un octet d'échappement* (ESC) avant le faux fanion pour éviter la confusion avec un *vrai* fanion
- méthode OK mais liée à l'emploi de caractères codés sur 8 bits, or UNICODE, par ex., code sur 16 bits

Couche LdD : Trames

- recherche d'une technique permettant de traiter des caractères de taille quelconque:

– utilisation d'indicateurs de début et fin de trame en remplissant des *bits*

- chaque trame commence et finit par 01111110
- si la couche LdD détecte 5 bits à 1 consécutifs (risque de confusion avec le fanion), elle *insère* à leur suite un *bit à 0*
- ex. :

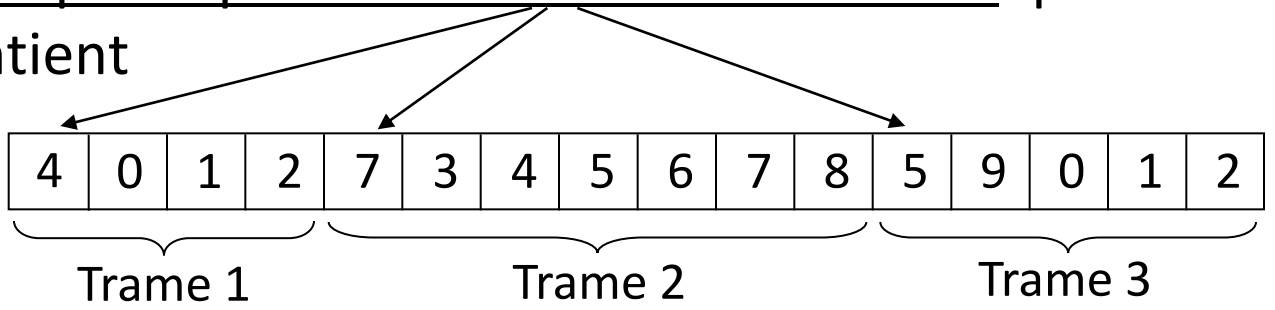
01110101111111110001

01110101111**0**11111**0**0001

Bits de remplissage (ou de transparence)

Couche LdD : Trames

- Comptage des caractères
  - la couche LdD ajoute dans l'entête de la trame un champ indiquant le nombre de caractères qu'elle contient



  - problèmes gênants en cas d'erreurs (lesquels ?)

  => cette méthode est souvent utilisée en complément d'une des autres précédemment citées

Couche LdD: fonctions de contrôle

- Contrôle d'erreur
  - **acquittement** (= trame de contrôle) positif ou négatif envoyé par le récepteur à l'émetteur
  - utilisation de **timers** pour éviter les attentes infinies de l'émetteur
  - **numérotation** des trames pour éviter les confusions entre trames originales et trames réémises

  ☙*NB: acquittements, numérotations… impliquent un mode point à point et non un mode diffusion*

Couche LdD: fonctions de contrôle

- Contrôle de flux
  - lorsque le récepteur est moins rapide que l'émetteur, il perd des trames, même si elles ont été transmises sans erreurs
  - 2 approches:
    - fondée sur le débit (*rate based flow control*) : limitation du débit de transmission des données (non utilisée ds la couche LdD, mais ds les couches supérieures)
    - rétroaction (*feed-back based flow control*) : interdiction à l'émetteur d'envoyer des trames tant qu'il n'a pas de feu vert du récepteur

Couche LdD : Erreurs de transmission

- 2 solutions:
  - introduire bcp de redondance ds les données pour que le récepteur puisse *corriger* l'erreur
    - => codes correcteurs d'erreurs
    - utilisation : canaux peu fiables (ex. réseaux sans fil)
  - introduire un peu de redondance ds les données pour que le récepteur puisse *détecter* l'erreur
    - => codes détecteurs d'erreurs
    - utilisation : canaux fiables (ex. fibre optique)

Couche LdD : Erreurs de transmission

- Trame: *n* bits = *m* bits de données + *r* bits redondants
- **mot de code** : l'ensemble des *n* bits
- Détermination du nombre de bits différents entre 2 mots de code à l'aide d'un ***ou exclusif*** (XOR) puis comptage des 1 : c'est la *distance de Hamming*
- Ex: 11000101 XOR 10001101 ???

Couche LdD : Hamming

- Soient *M* et *M'* deux mots de code avec une distance de Hamming *d*
  - il faut *d* erreurs simples pour que *M* devienne *M'*
- Soit *C* un code composé de *N* mot valides
  - La distance de Hamming de ce code est la *distance minimale* qui sépare deux mots valides
  - Exemple : *C*= [000000, 001110, 010101, 011011, 100011, 101101] Que vaut *d* ?
- **Un code avec une distance *d* détecte *d*-1 erreurs et corrige *k* erreurs où *d*=2*k*+1**

Couche LdD : bit de parité

- Autre exemple de code détecteur: ***code de contrôle de parité*** (paire ou impaire)
- Pour une parité paire (impaire), on protège la chaîne de bits en ajoutant 1 bit de sorte que le nombre de bits à 1 soit pair (impair)
- Que vaut *d* pour ce code ?
- Ex: `10011 ==> 10011`**`1`**

  (parité paire)

Couche LdD : CRC

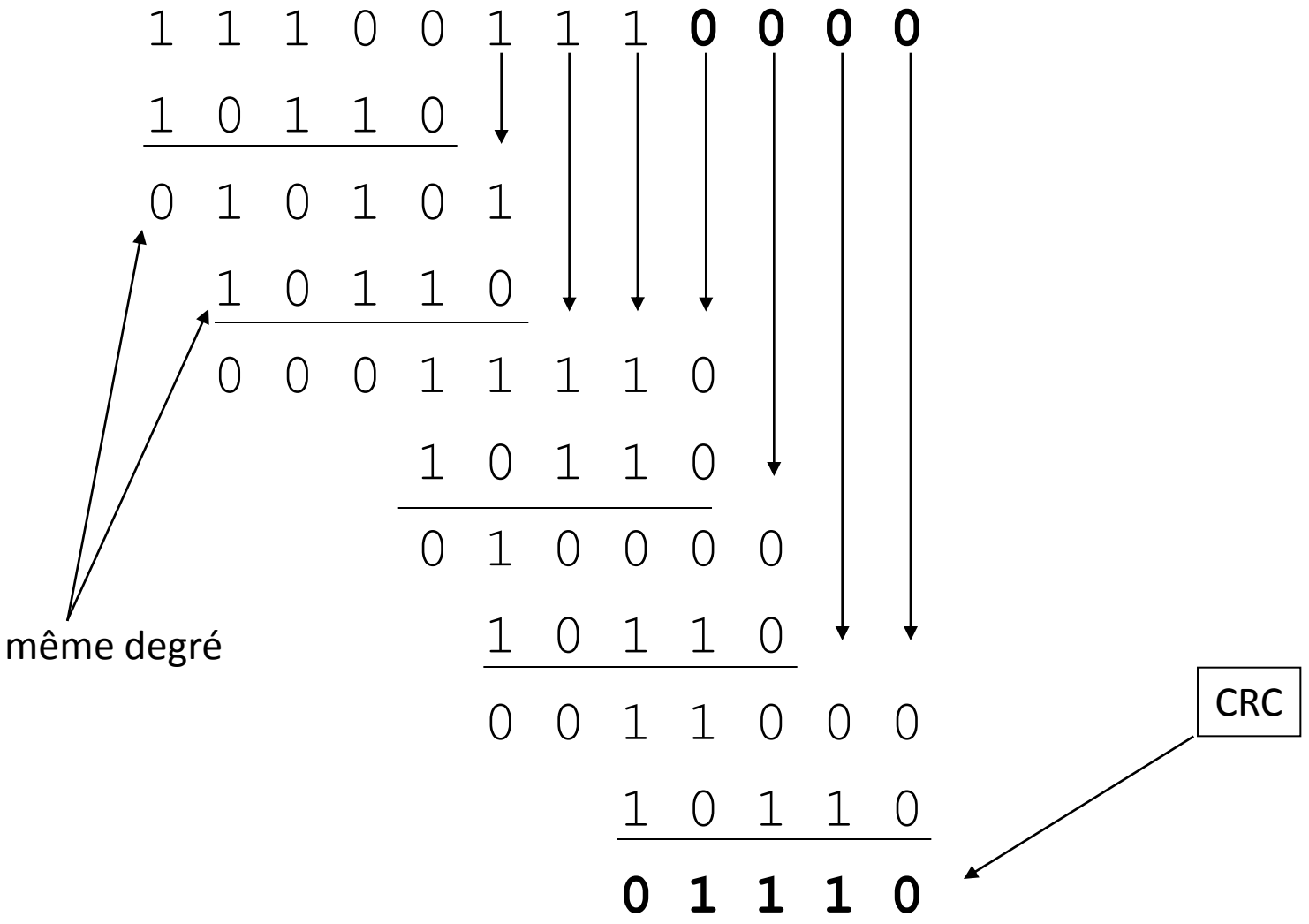
- autre code détecteur: ***code de redondance cyclique*** (CRC)
- les bits à transmettre sont considérés comme les coeff. d'un polynôme
- division modulo 2 (XOR successifs) de ce polynôme par un *polynôme générateur*
- le reste de la division binaire constitue le CRC
- CRC est ajouté à la suite des bits à transmettre.
- A la réception, division du polynôme formé par les bits reçus par le polynôme générateur : si ce CRC obtenu est nul, alors *pas d'erreur*

Couche LdD : CRC

- Exemples de polynôme générateur G(x):
  - $x^{16}+ x^{12} + x^5 + 1$: dans X25
  - x^8+x^2+x+1: ATM
- Technique à l'aide d'un exemple
  - Mot à transmettre: 11100111 avec G(x) = x^4+x^2+x
  - G(x) = $1\times x^4 + 0 \times x^3 + 1\times x^2 + 1\times x^1+ 0\times x^0$

  ☙ => 1 0 1 1 0
  - degré de G(x) = 4 => ajout de 4 zéros au mot => 1110011**0000**
  - puis division du mot par G(x) => additions binaires sans retenue (XOR) entre le mot à transmettre (puis le résultat de l'addition) et G(x)
  - les sommes se font entre 2 mots (polynômes) de ***degré égal***

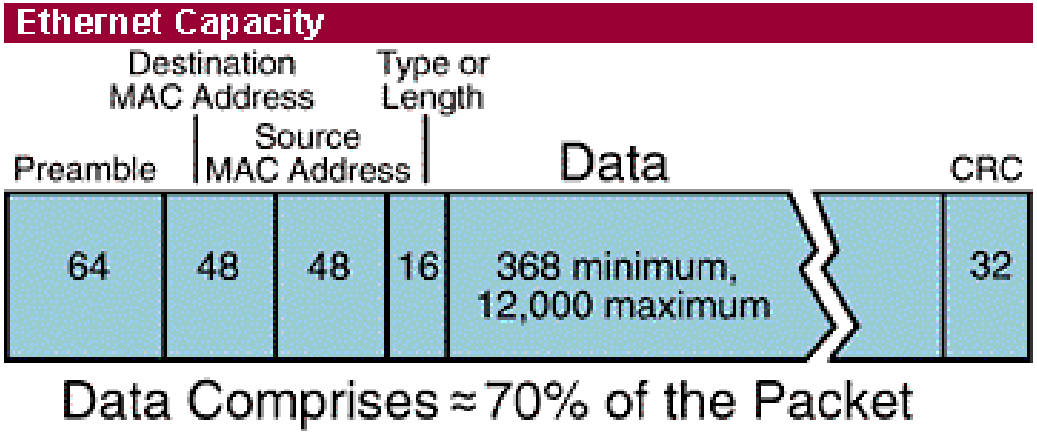
Couche LdD : CRC



=> transmission du mot + CRC, soit : 11100111 1110

Couche LdD : CRC

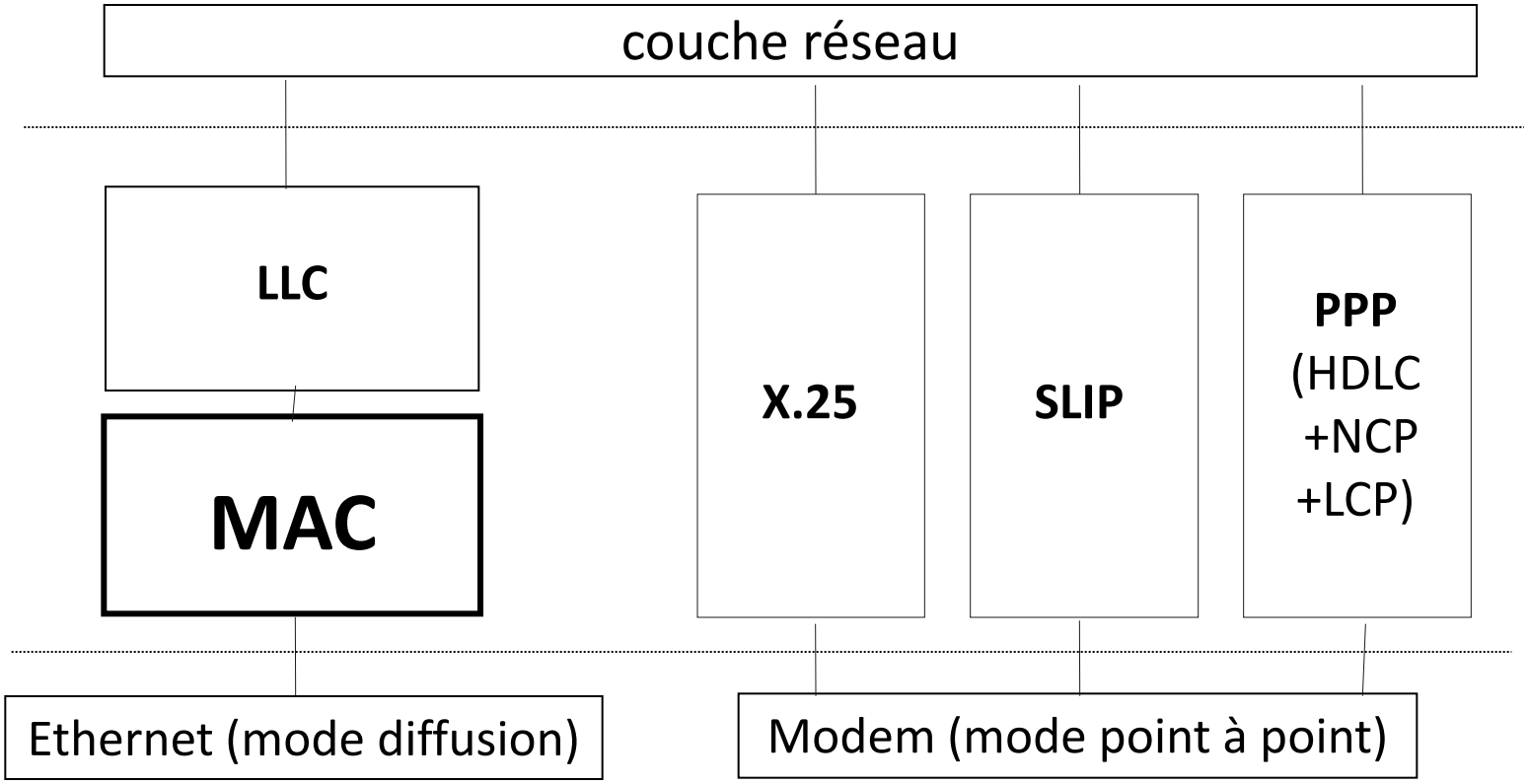
- Ethernet (IEEE 802.3) utilise le CRC:



  - préambule: pour la synchronisation
  - adresses MAC: adresses physiques (uniques) des cartes
  - longueur ou taille des informations reçues de la couche LLC
  - données utiles issues de la couche LLC

Sous couche MAC

- MAC (Medium Access Control) constitue la sous-couche basse de la couche Liaison de Données



Sous couche MAC

- But de cette sous-couche:
  - allouer le (seul) canal de diffusion que se partagent plusieurs stations:
    - allocation statique
    - allocation dynamique
  - gérer les accès concurrents sur le canal
- MAC joue un rôle important pour les LAN principalement
- *Rappel: ici, les transmissions se font en mode diffusion (broadcast)*

Sous couche MAC: Allocation

- Allocation statique d'un canal
  - multiplexage en fréquence (FDM)
    - division du canal en *n* sous-canaux (1 par utilisateur)
    - division de la bande passante en *n* portions de même taille
    - => pas d'interférences entre les communications
  - multiplexage temporel (TDM)
    - allocation d'un espace de temps fixe qui se renouvelle tous les *N* intervalles de temps

  => Avantages, inconvénients ?

Sous couche MAC : Allocation

- Problèmes (BP sous-utilisée; + de *n* utilisateurs ??) si
  - nb d'utilisateurs important
  - nb d'utilisateurs varie ds le temps
  - => trafic en rafales courtes et espacées
- Solution: allocation dynamique
  - nombreuses méthodes:
    - ALOHA
    - CSMA
    - …

Sous couche MAC : Allocation

- Allocation dynamique d'un canal
  - *N* utilisateurs pour 1 canal unique
    - toutes les stations sont équivalentes
  - Gestion des collisions
    - collision : envoi de plus d'une trame simultanément
  - Gestion du temps
    - émission n'importe quand (temps continu)
    - émission dans un intervalle de temps IT (temps discrétisé)
  - Détection de porteuse (*Carrier Sense*)
    - vérification de la disponibilité du canal avant émission

Sous couche MAC: Protocoles

- ALOHA
  - 1970, université d'Hawaï (N. Abramson)
  - initialement, pour un réseau de stations radio terrestres
  - 2 versions:
    - ALOHA pur: pas d'IT => transmission sans réserves
    - ALOHA discrétisé: présence d'IT
      => synchronisation sur les IT

Sous couche MAC: Protocoles

- ALOHA pur
  - liberté pour la transmission : utilisateurs peuvent envoyer leurs données **quand ils le veulent**
  - détection de collisions par **écoute** et **retransmission** différée avec délai aléatoire (*pourquoi?*)
  - => systèmes à **contention**
  - rendement de ALOHA pur est optimal lorsque toutes les trames sont de même taille
  - taux d'occupation du canal assez faible (taux maximum: environ 18 %)

Sous couche MAC: Protocoles

- ALOHA discrétisé (slotted ALOHA)
  - 1972 (Roberts)
  - fondée sur la synchronisation des transmissions avec IT (IT = *slot*)
  - nécessité d'avoir une station qui joue le rôle d'horloge
  - permet de doubler la capacité de transmission => taux d'occupation max d'environ 36 %

Sous couche MAC: Protocoles

- CSMA (*Carrier Sense Multiple Access*)
  - *Protocoles à **détection de porteuse**: écoute **avant** d'émettre*
  - Plusieurs protocoles dans cette famille: CSMA persistant et non persistant, CSMA/CD
  - CSMA *1-persistant*
    - écoute du canal avec attente de libération et émission immédiate (si collision, retransmission différée avec temps aléatoire)
    - taux d'occupation du canal: environ comme ALOHA discrétisé

Sous couche MAC: Protocoles

- CSMA *non persistant*
  - écoute du canal, si celui-ci est occupé, écoute différée après un temps aléatoire (émission sur une écoute de canal libre)
  - donc pas d'écoute permanente
- CSMA *p-persistant*
  - utilisation des IT
  - après une écoute avec attente, probabilité *p* d'émission immédiate et 1-*p* d'émission à l'IT suivant

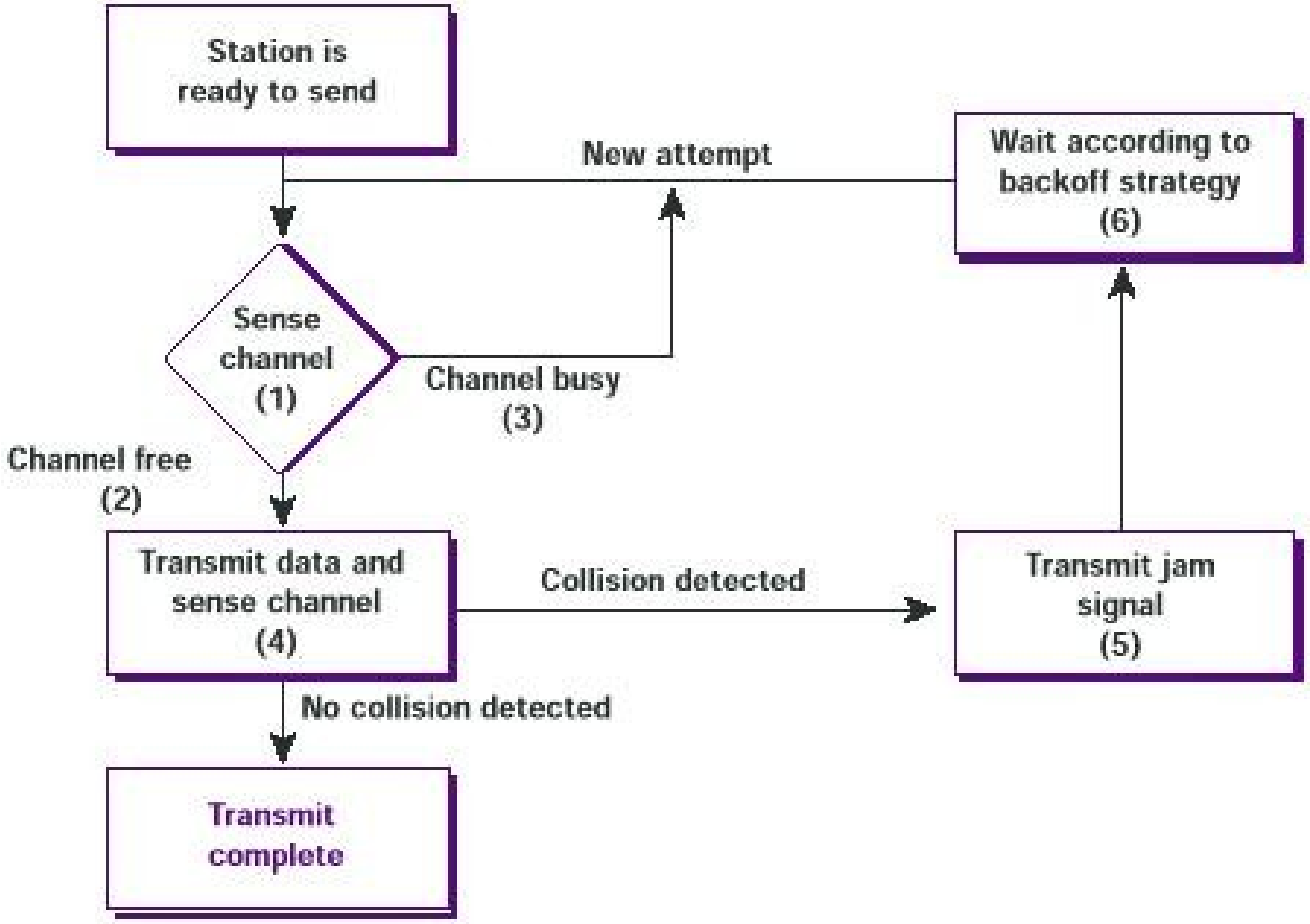
Sous couche MAC: Protocoles

- CSMA/CD (*CSMA with Collision Detection*)
  - Améliorations des CSMA précédents:
    - arrêt d'émission immédiat si collision (la trame n'est donc pas transmise dans son intégralité)
    - ↬ => gain en temps et bande passante
    - périodes de **contention** pendant lesquelles les stations tentent d'émettre (envoi de « bouts » de trames)
    - plus de collisions pendant l'émission des données
    - en cas de collision, chaque station impliquée déroule un algorithme de reprise
  - *NB*: Ethernet (norme IEEE 802.3) fonctionne en CSMA/CD. C'est le transceiver qui s'occupe du CD

Sous couche MAC: Protocoles

- CSMA/CD: Vocabulaire
  - séquence de brouillage (*jam sequence*)
    - séquence de brouillage envoyée par une station dès qu'elle a détecté une collision, afin de la rendre détectable par l'ensemble des stations impliquées
  - tentative (*attempt*)
    - tentative d'émission d'une trame. Si ce nombre est trop élevé, alors "erreur de collision"
  - délai (*backoff strategy*)
    - calcul d'un délai aléatoire

Sous couche MAC: Protocoles



CSMA/CD Flow Chart

Sous couche MAC: Protocoles

Protocoles sans collision

- objectif: libérer le canal de toute collision, même pendant la période de contention

- ex: Protocole Bit-Map

méthode de liste binaire (pour les adresses des stations)

•chaque période de contention contient *N* ***slots*** (avec *N*: nb de stations)

•réservation pour l'émission des prochaines trames:

ex: si station n°0 veut émettre, elle émet un 1 pendant le slot 0

•Seule la station n°*i* a le droit d'émettre pendant le slot *i*

•A la fin des *N* slots, toutes les stations ont connaissance de l'ordre de passage et la transmission se fait sans collision

Sous couche MAC: Protocoles

Allocation dynamique à accès déterministe

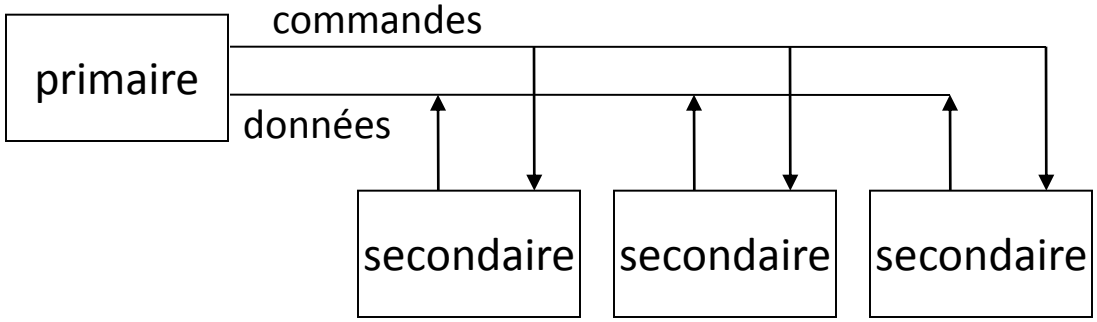
contrairement à l'accès aléatoire, ici, les stations ont la parole à tour de rôle

3 méthodes:

- accès par polling (centralisée)
- accès par jeton non adressé sur un anneau (décentralisée)
- accès par jeton adressé sur un bus (décentralisée)

Sous couche MAC: Protocoles

Accès par *polling* (= invitation à émettre)



station primaire:

gère l'accès grâce à une table de scrutation

relaie les trames vers les secondaires (topo: *étoile*)

station secondaire:

transmission des trames autorisées par la primaire

réception des autres trames

Sous couche MAC: Protocoles

Accès par jeton non adressé sur anneau

- jeton donne droit à transmettre une trame
- topologie en anneau: sens unique de parcours
- jeton: séquence binaire (trame) spéciale
- trame de type HDLC
- norme IEEE 802.5 : anneau à jeton d'IBM (*Token ring*)
- réseau FDDI (*Fiber Distributed Data Interface*) => réseau LAN en fibre optique qui utilise la technique d'anneau à jeton

Sous couche MAC: Protocoles

Accès par jeton non adressé sur anneau (suite)

- principe: (jeton circule librement sur anneau)

émetteur:

- attraper le jeton
- transmettre ses trames d'information (pdt une durée fixée)
- attendre le retour de cette trame et la retirer de l'anneau
- retransmettre le jeton sur l'anneau

récepteur:

- si trame est jeton alors passer au voisin
- sinon, si trame d'information qui arrive lui est destinée, alors copie dans un buffer puis retransmission de la trame, sinon retransmission sans copie

Sous couche MAC: Protocoles

Accès par jeton adressé sur bus

- topologie physique en bus => double sens de parcours
- établissement d'un anneau virtuel grâce aux adresses des stations précédentes et suivantes stockées dans chaque station
- gestion de l'anneau virtuel:
  - des stations peuvent vouloir rejoindre l'anneau ou le quitter
  - => périodiquement, la station ayant le jeton envoie une trame de *RechercheSuccesseur* pour modifier (si besoin) la structure de l'anneau

Sous couche MAC: Protocoles

- Accès par jeton adressé sur bus (suite)
  - trame de type HDLC
  - Norme IEEE 802.4 : bus à jeton (Token bus)
  - Principe:
    - le jeton parcourt cet « anneau » virtuel
    - émetteur attend le jeton adressé par la station précédente, transmet son information puis passe le jeton à son successeur
    - récepteur vérifie si trame d'information est pour lui (il la copie alors) et la passe, dans tous les cas, à son successeur

NB: Fin des rappels réseaux filaires

Couche MAC du 802.11

Introduction

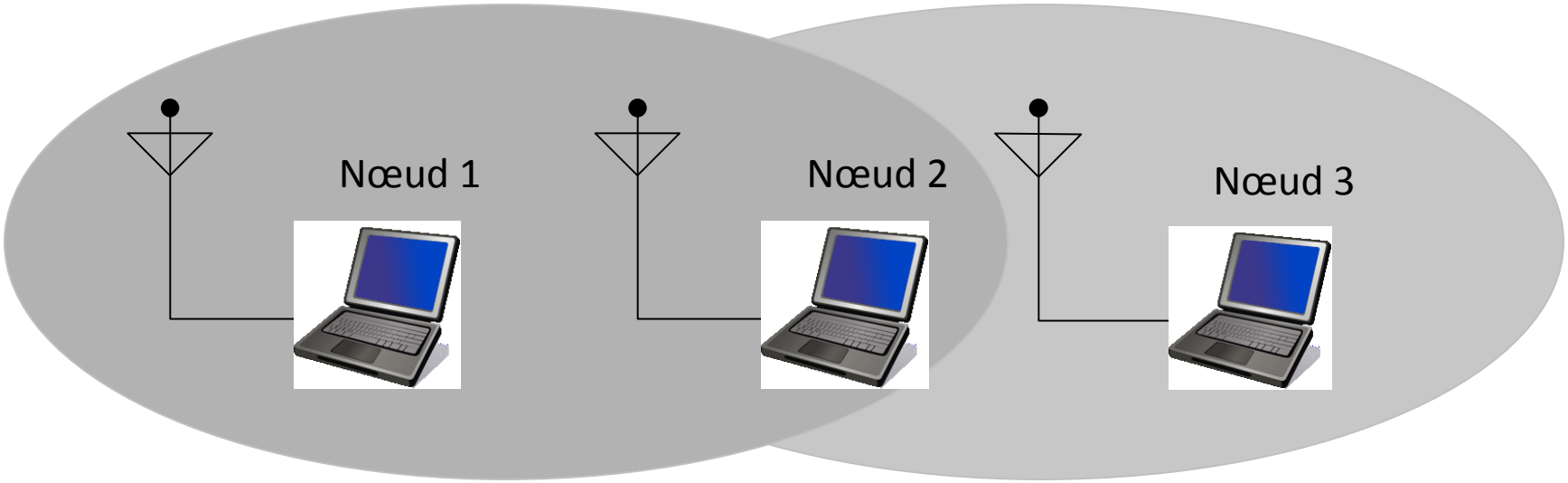
- Cette couche est l'élément clé de la spécification du 802.11
- Elle contrôle la transmission des données
- Elle fournit la base des opérations de manipulation des trames + l'interaction avec un DS filaire
- Elle utilise un CSMA/CA (càd un CSMA avec Collision Avoidance, qui tente d'éviter les accès simultanés (donc les collisions) en retardant l'accès au médium).

Couche MAC du 802.11

- Principales différences entre CSMA/CD (Ethernet) et CSMA/CA (802.11)
  - Medium = ondes radio, donc qualité nécessairement moins bonne que le filaire (pb de portée, d'interférences…)
  - => toutes les trames doivent être acquittées (ACK positifs)
  - => chaque échange de trame est de type « tout ou rien » (soit tout se passe bien, soit tout se passe mal. Cf. schéma d'un échange)
  - Bien sûr, chaque envoi est soumis au mécanisme d'écoute de la porteuse.

Couche MAC du 802.11

- Problème dit du « nœud caché »
  - Frontières d'un réseau sans fil sont floues : tous les nds ne peuvent pas tjs communiquer avec tous les autres nds du même réseau.



  - D'où utilisation de signaux de Demandes pour émettre (RTS : Request To Send) et Prêt à émettre (CTS : Clear To Send) pour dégager une aire

Couche MAC du 802.11

- Coordination et minutage du MAC
  - 3 types de fonctions de coordination :
    - DCF (Distributed Coordination Function, Fonction de coordination distribuée) : base du mécanisme CSMA/CA standard. L'évitement des collisions se fait avec un backoff (ralentissement) aléatoire après chaque trame
    - PCF (Point coord. Function, Fonction de coordination par point) : fournit des services sans contention. Des coordinateurs de points (stations spécifiques) sont utilisés pour garantir la non contention. (uniquement sur BSS infrastructure). Minutage rigoureux. Peu mise en œuvre.
    - HCF (Hybrid Coord. Func) : (cf. norme 802.11e, novembre 2005). Entre PCF et DCF. Cf. mode EDCA (Enhanced Distributed Channel Access) qui définit 4 catégories d'accès au medium :
      - priorité à la voix ;
      - priorité à la vidéo ;
      - priorité dite "Best Effort" pour les applications standard ;
      - priorité dite "Background" lorsque le trafic est faible.

Couche MAC du 802.11

- Ecoute de porteuse et allocation
  - 2 types d'écoute :
    - Physique : fonctions fournies par la couche physique (souvent coûteux)
    - Virtuelle: fournie par le vecteur d'allocation réseau (NAV) => minuterie indiquant la durée pdt laquelle le medium sera réservé (en microsecondes). NAV fixé par les stations. Qd NAV >0, medium est occupé. Sinon medium inactif. NAV intéressant pour s'assurer que les opérations atomiques ne seront pas interrompues.

  Schéma :

Couche MAC du 802.11

- Intervalles inter-trames
  - Il en existe 4 différents, en fonction du niveau de priorité des trafics : SIFS, PIFS,DIFS, EIFS
    - SIFS : short IFS : utilisé pour les transmissions dont la priorité est la plus élevée
    - PIFS : PCF IFS : utilisé par la PCF (pdt une opération sans contention)
    - DIFS : DCF IFS : utilisé par la DCF
    - EIFS : extended IFS : intervalle non fixe. Utilisé seult en cas d'erreur ds l'émission d'une trame.
- Accès avec contention utilisant la DCF
  - Avant de démarrer une transmission, chq station vérifie si médium inactif
  - Si medium inactif depuis + longtps que le DIFS, transmission peut commencer (principe du NAV)
    - Si trame précédente a été reçue sans erreur, medium doit être libéré pdt au moins la durée du DIFS
    - Si trame préc. contenait erreur, medium doit être libérée pdt durée EIFS
  - Si medium occupé, stations emploient un algo de ralentissement exponentiel => « ajournement d'accès »

Couche MAC du 802.11

- Reprise sur erreur avec la DCF
  - Chaque trame (ou fragment) a un cpt de tentatives associé (cf. Ethernet où le mécanisme est le même).
  - Il y a 2 types de cpt : court (typiquement, pour trames inférieures au NAV RTS) et long (trames sup. seuil RTS)
  - Cpt court est remis à zéro si :
    - Trame CTS est reçue en réponse à un RTS *ou*
    - Un ACK est reçu *ou*
    - Trame à diffusion générale ou multiple est reçue
  - Cpt long est remis à zéro si :
    - Un ACK est reçu pour une trame plus longue que seuil RTS *ou*
    - Trame à diffusion générale ou multiple est reçue
  - Notion de « durée de vie » maximum pour chaque fragment : à chaque émission d'un fragment, ce cpt est démarré. Lorsqu'il atteint son max, trame est annulée et fragments restants ne sont pas transmis

Couche MAC du 802.11

- Ralentissement d'accès avec la DCF
  - Fenêtre de contention (ou fenêtre de ralentissement) suit le DIFS.
  - Elle est divisée en slots.
  - La taille d'un slot dépend du medium
  - Les stations choisissent un slot aléatoire et attendent la fin de la fenêtre avant de retenter d'accéder au médium.
  - Chaque slot a la même proba d'être tiré au sort
  - La durée du ralentissement est sélectionnée dans une plage plus importante chaque fois qu'une transmission échoue (durée exponentielle)

  Schéma :

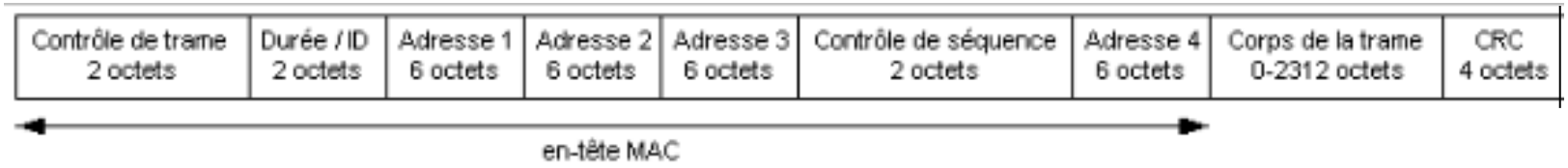
Couche MAC du 802.11

- Fragmentation et réassemblage
  - Fragmentation nécessaire lorsqu'une trame est trop longue.
  - Les fragments ont tous meme numero de sequence de trame, mais des numéros de fragment croissants
  - Rafale de fragments : grâce au SIFS et au NAV, on est sûr que d'autres stations n'utiliseront pas le canal pdt l'échange.

Schéma :

Couche MAC du 802.11

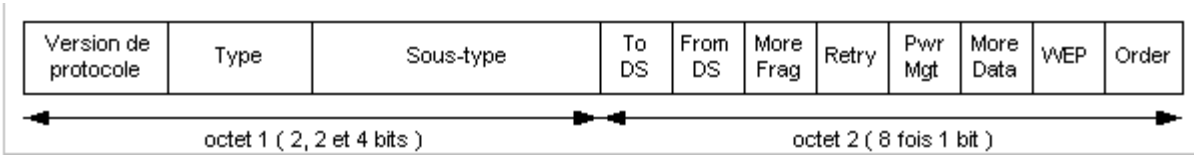
- Format d'une trame
  - trois sortes de trames :
    - trames de données, (NB : les données sont la charge utile de la trame)
    - trames de contrôle utilisées pour l'accès au support (RTS, CTS, ACK…)
    - et les trames de gestion utilisées pour l'association à un point d'accès ou pour la synchronisation et l'authentification
  - La représentation de la trame est une représentation générale et ses champs changent suivant la fonction de celle-ci.
  - La taille maximale d'une trame est de 2347 octets (et minimum 34 octets)
  - **FORMAT GENERAL**



    - **En-tête** (7 champs sur 30 octets): C'est la partie la plus complexe car elle intègre de nombreuses fonctions

Couche MAC du 802.11

- **Contrôle de trame (11 sous-champs sur 2 octets):**



-Version de protocole : toujours à 0 pour la version actuelle (2 bits)

-Type et sous type : représente les 3 sortes de trames et leurs fonctions (2+4 bits)

-To DS et From DS : DS=Distribution Service (point d'accès).
To DS : (bit à 1) la trame est adressée au point d'accès pour qu'il la fasse suivre.
From DS (bit à 1) la trame vient du point d'accès.

-More Fragments : à 1 si les données sont fragmentées, à 0 si elles ne sont pas fragmentées ou s'il s'agit du dernier fragment (1 bit).

-Retry : à 1 s'il s'agit d'une retransmission (1 bit).

-Power Management : à 1 si la station est en mode d'économie d'énergie, à 0 si elle est active (1 bit). Venant du point d'accès, les trames sont toujours en mode actif.

Couche MAC du 802.11

- **Contrôle de trame (suite)**

  -More Data : 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 (1 bit).

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

  -Order : si à 1 cela indique que la trame est envoyée en utilisant une classe de service strictement ordonné. Ne permet pas à la station d'envoyer des trames en multicast.

  Durée/ID (2 octets) :

  Ce champ a deux sens, dépendant du type de trame :
  - pour les trames de polling en mode d'économie d'énergie, c'est l'ID de la station ou AID (Association IDentity)
  - dans les autres trames, c'est la valeur de durée utilisée pour le calcul du NAV.

Couche MAC du 802.11

- **Champs adresses (4 fois 6 octets) :**

  L'adresse MAC de 48 bits se décompose en trois parties
  -un groupe de 2 bits au début de adresse : le premier indique si l'adresse est individuelle (bit à1) ou de groupe (bit à 0), le deuxième indique si l'adresse est locale (bit à 1) ou universelle (bit à 0). Si l'adresse est locale, les 46 bits suivants sont définis localement.
  -un groupe de 22 bits : numéro constructeur défini par l'IEEE
  -un groupe de 24 bits : numéro de série défini par le constructeur

  Adresses de groupe :
  -adresse broadcast : définit l'ensemble des stations du réseau. (les 48 bits sont à 1)
  -adresse multicast : définit un groupe de stations en nombre fini.

  Types d'adresse :
  La structure d'adressage 802.11 est plus riche que pour un réseau filaire. Car si on veut accéder à une station du même réseau (BSS), il faut passer par le point d'accès donc indiquer son adresse MAC pour qu'il relaie le paquet. De même pour accéder à une station d'un autre réseau (ESS), deux adresses intermédiaires peuvent être indiquées. Ces champs d'adresses sont définis en accord avec les indications des champs To DS et From DS.

Couche MAC du 802.11

- **Champs adresses (suite) :**
  - Quatre types d'adresse et 5 utilisations en tout:
    - BSSID (Basic Service Set Identifier):
      rappels : En mode infrastructure -> @ MAC du PA ; En mode Ad-Hoc -> @ MAC locale du BSSID (générée lors de la création de l'IBSS)).
    - DA (Destination Address) : adresse, individuelle ou de groupe, identifie le(s) destinataire(s).
    - SA (Source Address) : adresse individuelle ayant transmis la trame.
    - RA (Receveir Address) : BSSID destination (point d'accès récepteur).
    - TA (Transmitter Address) : BSSID source (point d'accès émetteur).

ToDS	FromDS	@1 destination Récepteur	@2 source Emetteur	@3 sce initiale dest finale	@4 WDS*	ETAPE
0	0	DA	SA	BSSID	---------	0
1	0	BSSID	SA	DA	---------	1
0	1	DA	BSSID	SA	---------	2
1	1	RA(BSSID)	TA(BSSID)	DA	SA	3

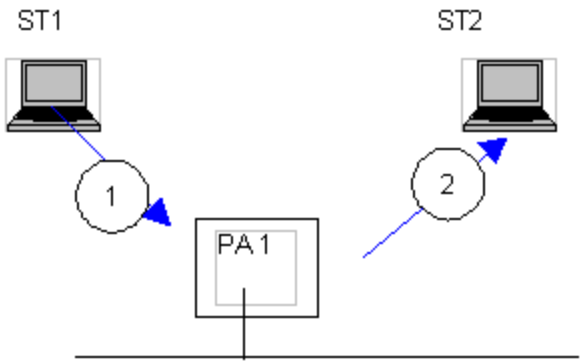
*Wireless Distribution Service (liaison entre deux AP)

Couche MAC du 802.11

- **Champs adresses (suite) :**
  Exemple d'adressage:

  Le mode Ad-Hoc : transmission dans un IBSS, ST1 envoie ses données vers ST2.
  Etape 0: @1: ST1, @2: ST2, @3: BSSID de l'IBSS.

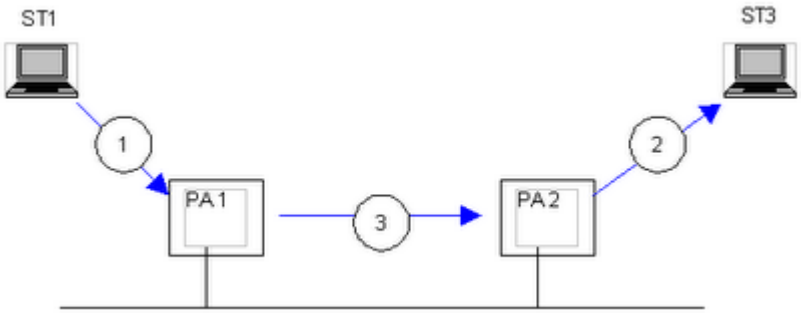
  Le mode infrastructure :
  -<u>1er Cas :</u> transmission dans un même BSS, ST1 envoie ses données vers ST2 (via PA1).
  Etape 1 : ST1 envoie la trame vers PA1 pour destination finale ST2.
  To DS: à 1, @1 : PA1 (dest); @2 : ST1 (sce), @3 :ST2 (dest finale).



  Etape 2 : PA1 envoie la trame vers ST2.
  From DS à 1, @1 : ST2 (dest), @2 : PA1, @3 : ST1 (sce initiale).

Couche MAC du 802.11

- **Champs adresses (suite) :**
  Le mode infrastructure (suite) :
  -2e Cas: transmission dans un même ESS, ST1 envoie ses données vers ST3 (via PA1 et PA2).
  A la différence de l'exemple précédent, l'étape 3 suit l'étape 1.
  Etape 3 :PA1 envoie la trame vers PA2
  To DS et From DS sont à 1, @1 : PA2 (dest), @2 : PA1 (sce), @3 :ST3, @4 : ST1.



- **Contrôle de séquence (2 octets) :**
  -numéro de séquence (12 bits) : numéro assigné à chaque trame.
  -numéro de fragment (' bits) : numéro assigné à chaque fragment, si la trame est fragmentée.
- **Corps de la trame (données) (0-2312 octets)** : La taille peut être supérieure à 1500 octets à cause du chiffrement WEP. Il n'y a pas de données pour les trames de contrôle et de gestion.
- **FCS (Frame Check Sequence) (4 octets)** : CRC de 32 bits, pour le contrôle d'intégrité de la trame.

Couche MAC du 802.11

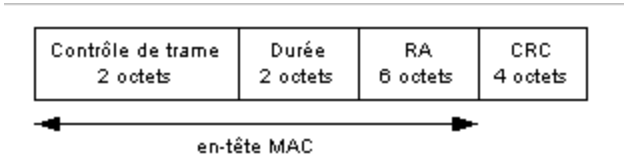
Cas des trames de contrôle

FORMAT TRAME DE CONTROLE :
Les trames de contrôle permettent l'accès au support et ont pour fonction d'envoyer les commandes et informations de supervision aux éléments du réseau. Dans la partie contrôle de trame, les champs de " ToDS " à " order " sont à 0.

·*Trames principales :*
a) RTS (Request to send) est utilisé pour réclamer le droit de transmettre une trame de données

-RA est l'adresse du récepteur destinataire de la prochaine trame de données ou de gestion.
-TA est l'adresse de la station qui transmet la trame RTS.

b) CTS (Clear To Send) correspond à la réservation du canal pour émettre une trame de données

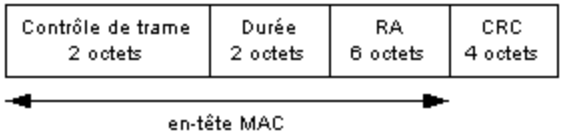


- RA correspond à l'adresse de la station source (champ TA) de la trame RTS.

Couche MAC du 802.11

FORMAT TRAME DE CONTROLE (suite)

c) ACK permet l'acquittement des trames de données



RA correspond à l'adresse de la station source, qui provient du champ adresse 2 de la trame de données ou de gestion précédente.

Cas des trames de Gestion

FORMAT TRAME DE GESTION :

Il existe quatre familles de trames de gestion :
·Trames liées aux fonctions d'association-désassociation
·Trames d'interrogation du voisinage radio
·Trames liées aux fonctions d'authentification
·Trames balises, utilisées par le point d'accès pour diffuser des informations dans le BSS, gestion du mode économie d'énergie grâce aux balises TIM et DTIM.

Couche MAC du 802.11

FORMAT TRAME DE GESTION (suite) :

Valeur du type (b3 b2)	Description du type	Valeur du sous-type (b7 b6 b5 b4)	Description du sous-type
00	Gestion	0000	Requête d'association
00	Gestion	0001	Réponse d'association
00	Gestion	0010	Requête de ré-association
00	Gestion	0011	Réponse de ré-association
00	Gestion	0100	Demande d'enquête
00	Gestion	0101	Réponse d'enquête
00	Gestion	0110-0111	Réservés
00	Gestion	1000	Balise
00	Gestion	1001	ATIM
00	Gestion	1010	Désassociation
00	Gestion	1011	Authentification
00	Gestion	1100	Désauthentification
00	Gestion	1101-1111	Réservés
01	Contrôle	0000-1001	Réservés
01	Contrôle	1010	PS-Poll
01	Contrôle	1011	RTS
01	Contrôle	1100	CTS
01	Contrôle	1101	ACK
01	Contrôle	1110	CF End
01	Contrôle	1111	CF End et CF-ACK
10	Données	0000	Données
10	Données	0001	Données et CF-ACK
10	Données	0010	Données et CF-Poll
10	Données	0011	Données, CF-ACK et CF-Poll
10	Données	0100	Fonction nulle (sans données)
10	Données	0101	CF-Ack (sans données)
10	Données	0110	CF-Poll (sans données)
10	Données	0111	CF-ACK et CF-Poll (sans données)
10	Données	1000-1111	Réservés
11	Réservé	0000-1111	Réservés

Couche MAC du 802.11

PONTS : passage du 802.11 (sans fil) à Ethernet (filaire)

- Sans fil => filaire. Etapes :
  - Vérification de l'intégrité (FCS de la trame 802.11)
  - 2 cas :
    - Si les trames sont destinées à un AP (et non à une station ds le réseau ss fil, càd que l'AP sert de pont) rejet des trames qui n'ont pas le bon SSID
    - Détection et rejet des trames doublons (cf. fenêtres, ACK perdus…)
  - Déchiffrage de la trame (cf. chapitre sécurité)
  - Analyse de trame pr savoir si réassemblage nécessaire. Si c'est le cas et que c'est la dernière trame, *contrôle d'intégrité*
  - Si l'AP doit servir de PONT sans fil / fil (càd qd adresse3 ≠ adresse1 des champs @ de la trame), l'entête MAC sans fil est converti en entête MAC Ethernet (plus simple)
  - Le FCS est recalculé (même algo que pour Ethernet)
  - La nvelle trame est envoyée sur l'interface Ethernet.

Couche MAC du 802.11

PONTS (suite)

- Filaire => sans fil. Etapes :
  - Validation du FCS Ethernet
  - Un entête SNAP (Sub Network Access Protocol) est ajouté à la trame Ethernet
  - Planification de l'envoi de la trame : soit tout de suite, soit plus tard (cf. tampon de l'AP (l'AID du Durée/ID de la trame) pour les économies d'énergie)
  - Qd trame est placée dans file d'émission, elle reçoit un numéro de séquence. Protection éventuelle avec un code d'intégrité. Si fragmentation nécessaire, alors attribution d'un numéro de fragment
  - Chiffrement éventuel de la trame
  - Construction de l'entête MAC 802.11 (à partir de l'entête MAC Ethernet) => remplissage des adresses source et dest., du BSSID émetteur, etc.
  - Le FCS est recalculé
  - La nvelle trame est envoyée sur l'interface 802.11

Sécurité

- Quelques notions de base
  - Pour se protéger contre l'interception du trafic, CHIFFREMENT
  - Plusieurs normes, la 1ère était WEP (Wireless Equivalent Privacy) qui est à la base de TKIP
  - *Encryptage* : Données XOR *codons* = données chiffrées
  - *Décryptage* : données chiffrées XOR codons = données
  - Clef secrète est utilisée pour produire les codons (= flux de bits pseudo-aléatoires, cf. PRNG – Pseudo Random Number Generator)
  - Lorsqu'un flux de bits est *totalement* aléatoire, on parle de *masque jetable* => il s'agit d'un chiffrement dt il est mathématiquement prouvé qu'il est incassable par certains types d'attaques
  - Mais masque jetable est assez dur à réaliser. De plus, son usage unique le rend peu rentable...
  - RC4 permet d'obtenir un masque pseudo-aléatoire

Sécurité

- WEP : augmentation de la taille de la trame de 8 octets
  - WEP 64 bits utilise un IV (vecteur d'initialisation) de 3 octets et une clef de chiffrement de 5 octets (dont 4 pour l'ICV (integrity check value) qui est un CRC)
  - clef et IV forment une clef RC4 de 64 bits qui est à *usage unique* (grâce à l'IV)
  - Failles : lorsque le réseau est très actif, l'IV devient trop court et la clef est parfois réutilisée ; si clef utilisée est *proche*, WEP cassable ; fragmentation des paquets => cassage plus aisé
- 802.1X : standard (2002)
  - Fournit un cadre pour l'authentification et la gestion des clefs
  - Utilise EAP
- EAP (Extensible Authentication Protocol)
  - mécanisme d'identification universel
  - Fournit un protocole, càd qu'un échange de trames EAP spécifiques a lieu
  - EAP a été conçu pour être utilisé sur PPP

Sécurité

- Des faiblesses du chiffrement ds la couche LdD est né le 802.11i
  - Propose une *authentification* et un *chiffrement*
  - *Authentification* de l'utilisateur (ou station) sur l'AP (ex. 802.1X)
  - *Chiffrement* selon 3 protocoles
    - WEP (pour rétrocompatibilité)
    - TKIP (Temporal Key Integrity Protocol) : WEP amélioré
    - CCMP (Counter-Mode/CBC-Mac protocol) : alternative plus sûre que TKIP, CCMP est fondé sur AES (Advanced Encryption Standard)
  - WPA (WiFi Protected Access) est une norme commerciale qui spécifie TKIP et CCMP ; elle est née avant le 802.11i
  - WPA2 : est la version commerciale du 802.11i (chiffrement avec AES imposé)

Couche physique (PHY)

- 2 sous-couches : PLCP (Physical Link Convergence Procedure) et PMD (Physical Medium Dependent)
  - PLCP prépare les trames provenant de la ss-couche MAC :
    - ajoute son propre entête à la trame (champs pour la synchronisation notamment)
    - Passe les trames à la PMD
  - PMD peut ensuite procéder à la *modulation* pour l'envoi ds les airs
- 6 « couches » physiques : FH, DS, OFDM, HR/DSSS, ERP, PHY MIMO
  - utilisent la modulation par *étalement de spectre :*
    - Passer le + de signaux possible ds une bande la + étroite possible
    - l'émetteur utilise des fonctions mathématiques qui répartissent la puissance du signal sur de nombreuses fréquences ; le récepteur reconstitue le signal sur une bande étroite

Couche physique (PHY)

- FH (Frequency hopping) ou FHSS (FH Spread Spectrum)
  - Multiplexage par ***saut de fréquence*** : utilise plusieurs canaux répartis sur une large bande de fréquences
  - Changement rapide de fréquence de transmission selon un motif pseudo-aléatoire prédéterminé
  - Avantages :
    - résistance aux interférences,
    - signal plus difficile à intercepter,
    - Possibilité de partage de la bande de fréquence avec d'autres réseaux => utilisation plus efficace de la BP
  - Modulation par GFSK (Gaussian Frequency Shift Keying)
    - ex. avec GFSK à 4 niveaux, encodage du M

Couche physique (PHY)

- DS (Direct Sequence) ou DSSS (DS Spread Spectrum)
  - Multiplexage par étalement de spectre *à séquence directe* : utilise plusieurs canaux répartis sur une large bande de fréquences
  - Le signal est étalé sur une large bande de façon très contrôlée
    - signal est combiné avec un signal pseudo-aléatoire de fréquence beaucoup + grande
    - signal obtenu occupe donc une bande de fréquence + large, déterminée par la fréquence du signal pseudo-aléatoire
  - Modulation par DPSK (differential phase shift keying)
    - ex. avec DPSK à 4 états, encodage du M
  - Buts :
    - Rendre plus résistants aux brouillages les signaux occupant une bande de fréquences réduite
    - Permettre le partage de la même fréquence porteuse

Couche physique (PHY)

- OFDM (Orthogonal Frequency Division Multiplexing) - 802.11a
  - Méthode de découpage d'un large canal de fréquence en plusieurs sous-canaux utilisés en parallèle pour obtenir un débit élevé
  - débit théorique de 54 Mbps, portée d'environ 30 m
  - bande de fréquence utilisée : 5 GHz (largeur de canal : 20 MHz => plus de 30 canaux découpant la bande allant de 4,920 à 5,825 GHz)
  - Modulation multiporteuses par QAM (Quadrature Amplitude Modulation), BPSK (Bi-PSK : deux valeurs de phase possibles), QPSK (4 valeurs de phases)
  - codage par répartition en fréquences orthogonales sous forme de plusieurs sous-porteuses (utilisation de 8 canaux ne se recouvrant pas)
- HR/DSSS (High Rate DSSS) :
  - utilise le même système de canaux que le DSSS
  - possède une meilleure efficacité spectrale que le DSSS et permet d'offrir deux débits : 5.5 Mbit/s ou 11 Mbit/s.

Couche physique (PHY)

- ERP : variante du OFDM (802.11g) => adaptation de l'OFDM sur la bande des 2,4GHz
- PHY MIMO (Multiple Input Multiple Output) – 802.11n :
  - technologie des entrées-sorties multiples
  - Utilisation de plusieurs antennes émettrices/réceptrices pour améliorer la performance du système => traitement simultané des émissions et des réceptions
  - Largeur de canal de 40 MHz est utilisée pour la PHY
  - Cette fréquence utilise des bandes passantes plus larges => débits de données plus élevés