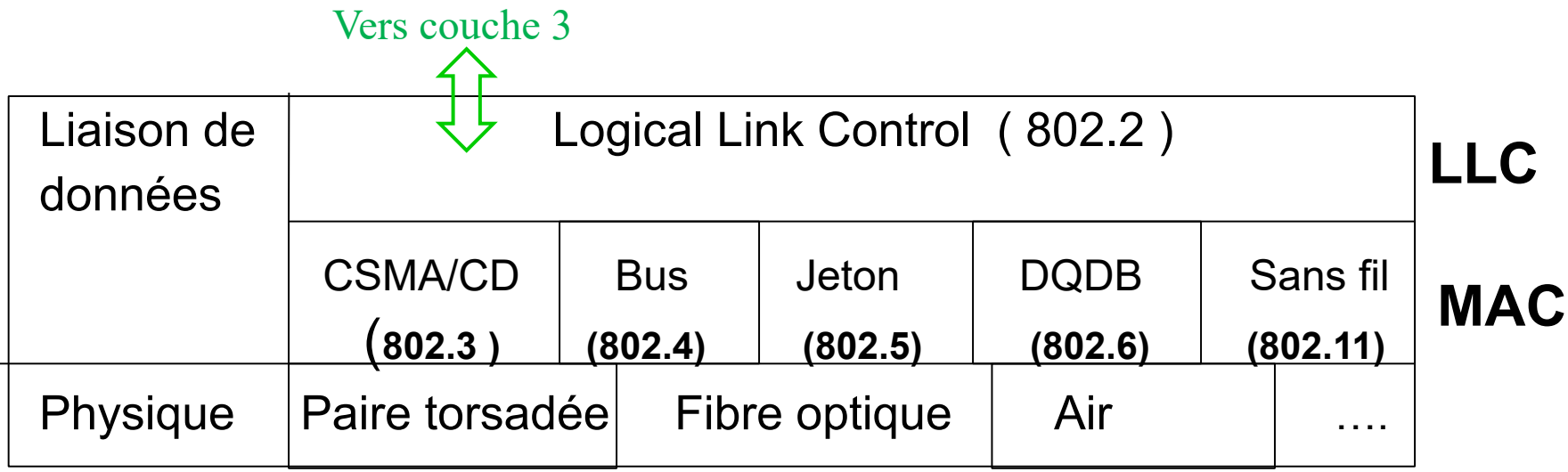
La Couche Liaison de données

La couche MAC - Généralité (1)

Transmission de bits entre systèmes raccordés sur le même réseau



MAC : Medium Access Control

En général, tout signal émis par l'un des systèmes raccordés peut être entendu par tous les autres

Équipement : switch, HUB, point d'accès

Couche 2 - Généralité

Les fonctionnalités de la couche 2

- Gestion des données
  - Problème : Repérage des différentes trames sur le support physique (suite de bits)

utilisation d'un fanion

- Détection et correction des erreurs
  - Numérotation des trames
  - Utilisation de code détecteur/correcteur d'erreurs

- Régulation du trafic
  - utilisation d'acquittement
  - Emission entre une source et un destinataire

Appellation unique de chaque entité MAC sur le médium

Identifie le système sur médium (le réseau local)

Appellation physique → adresse MAC

La couche MAC - Généralité (2)

Une entité-MAC par système

- reçoit les demandes d'émission (de la couche supérieure)
- décide quand émettre (méthode d'accès au médium)
- écoute ce qui est transmis, et décide de recevoir ou non

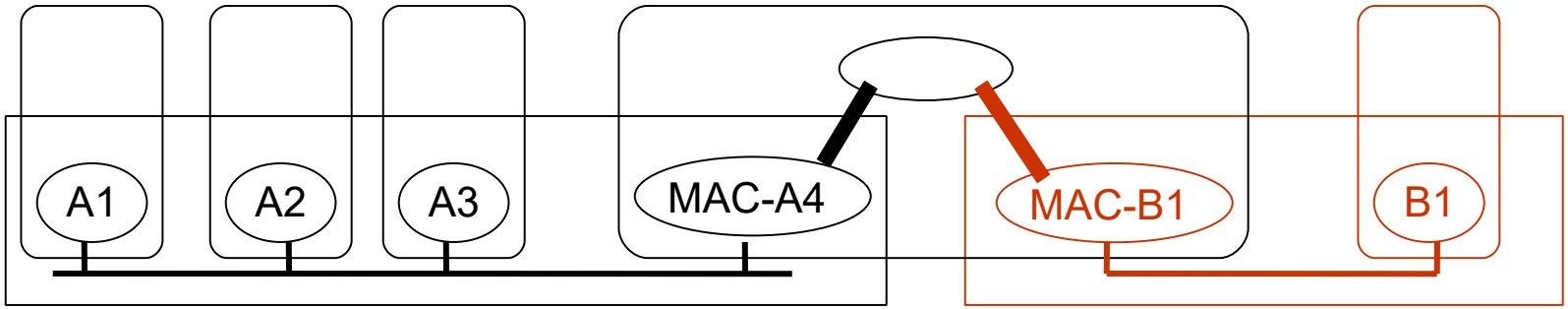
Si plusieurs couches MAC

Pas de communication entre deux couches MAC

Sauf si

un système est raccordé aux 2 supports et contient :

- une entité MAC pour chaque médium
- une entité-utilisateur de couches MAC liée à chacune des deux couches MAC ⇨ Routeur



L'adresse MAC

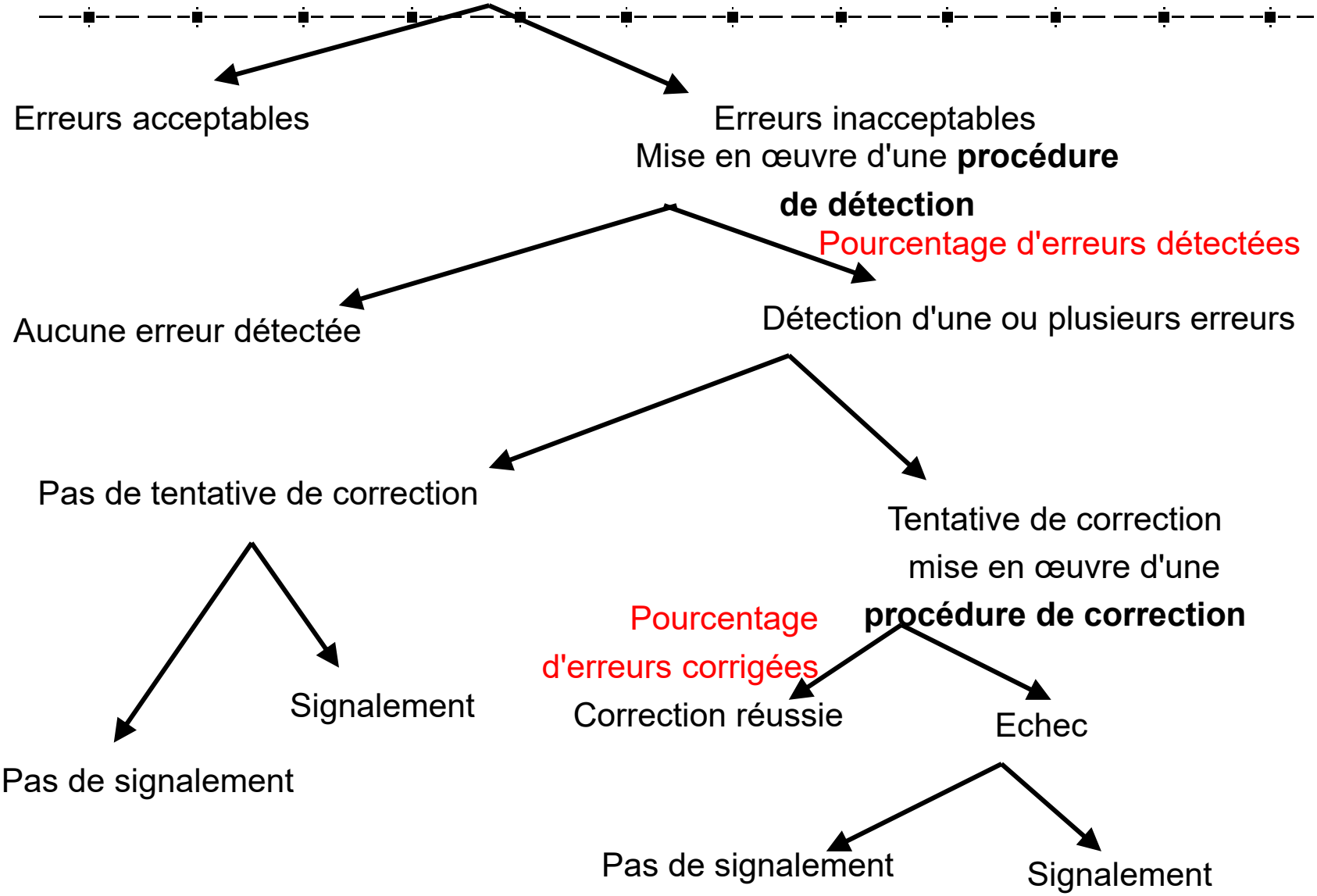
- Identification du niveau 2 :
  - **Unicité sur le médium/réseau local**
  - **adresse 6 octets**
    - 3 premiers octets :OUI (Organizationally Unique Identifier)
      - Concerne entreprise
    - 3 octets suivants : un numéro unique pour l'entreprise
    - Existe des @mac de groupe ou de broadcast

Tous les équipements réseaux communiquent en local grâce à leur adresse MAC (ou leur identifiant physique)

Test : ipconfig /all dans un shell windows : cmd

Traitement des erreurs

Stratégie de traitement d'une erreur



Code détecteur d'erreurs (1)

Contrôle de parité

- code VCR (Vertical redundancy Check)
- code LCR (Longitudinal Redundancy Check)

Codes Polynomiaux

- CRC : Cyclic Redundancy Check
- FCS : Frame Control Check

G(x) : polynôme générateur de degré r

M(x) : message à encoder

1100101 <-> $1*x^6 + 1*x^5 + 0*x^4 + 0*x^3 + 1*x^2 + 0*x^1 + 1*x^0$

<-> $x^6 + x^5 + x^2 + 1$

ex : $G(x)= x^{16} + x^{12} + x^5 + 1$ CRC-CCITT

$G(x)= x^8 + x^2 + x + 1$ ATM

$G(x)= x^{32}+ x^{26}+ x^{23}+ x^{22}+ x^{16}+ x^{12}+ x^{11}+ x^{10}+x^8+ x^7+ x^5+ x^4+ x^2+ x+1$ CRC-32-ethernet

Code détecteur d'erreurs (2)

Méthode

- On divise le polynôme $M(x)*x^r$ par $G(x)$ et on obtient le reste $R(x)$

  $M(x)*x^r = G(x)*Q(x) + R(x)$

- On envoie la séquence de bits de longueur $n=m+r$ tel que :

  $N(x)=M(x)*x^r + R(x)$

  - $N(x)$ est multiple de $G(x)$ car :

    $N(x)=M(x)*x^r + R(x) = G(x)*Q(x)+R(x)+R(x)$

    $= G(x)*Q(x)$

- On décode en faisant la division, le reste doit être nul

Mathématique en base 2 :

Addition

+	0	1
0	0	1
1	1	0

Soustraction

-	0	1
0	0	1
1	1	0

Exemple

- $G(x) = x^2 + 1$, → 101
- Message à envoyer : 1100 , c'est à dire $x^3 + x^2$

Division de $(x^3 + x^2) * x^2 = x^5 + x^4$ par le polynôme G(x)

```
1 1 0 0 0 0 | 1 0 1
0 1 1       | xxxx
  0 1 1     |
    0 1 1   |
      0 1 1 |
```

Reste 11

Message envoyé : 110011

```
Vérification : 1 1 0 0 1 1 | 1 0 1
                 0 1 1     |
                   0 1 1   |
                     0 1 0 |
                       0 0 0
```

Protocole de niveau 2

IEEE 802.3..., Ethernet -II

- Technique : CSMA/CD
  Carrier Sense Multiple Access / Collision Detection
- Topologie : Bus et maintenant maillage
- Méthode d'accès : par compétition

➡ Sur un bus :
(écoute du médium : si libre, émission
sinon attente)
Réémission après un temps d'attente si collision -> half-duplex

➡ Topologie maillée :
full-duplex → aucune collision possible, on émet immédiatement

- Débit :10 Mb/s, 100 Mb/s, 1 Gb/s, 10Gb/s

IEEE 802.3..., Ethernet -II

- Equipement :

  Half-duplex -> HUB

  Full-duplex → switch (commutateur)

- Trame :

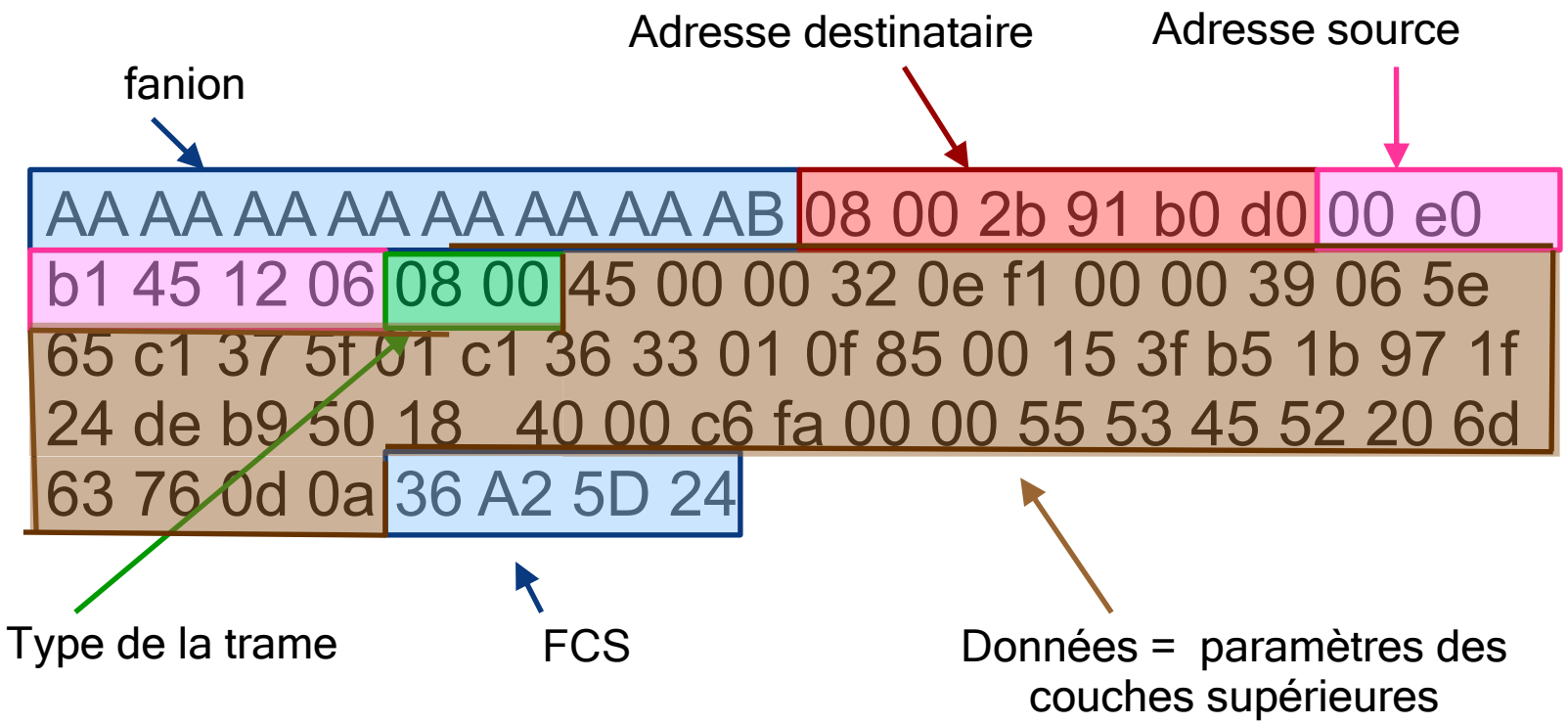
8 octets	6 octets	6 octets	2 octets	1 à 1500 octets	4 octets
Synchro	Adresse destinataire	Adresse expéditeur	type de trame / lg données	Données + bourrage	FCS

- Ethernet 802.3: lg données < 0x05DC

  Ethernet –II : protocole de niveau 3 encapsulé > 0x05DC

Exemple ethernet -II

Exemple d'une trame en hexadécimal :



Le fanion et le contrôle d'erreur (FCS) ne sont jamais représentés sauf ici.

La norme 802.11

La norme **802.11** définit la couche 1 et 2 pour une liaison sans fil utilisant des ondes électromagnétiques :

- La couche physique
  codage DSSS, FHSS, IrDA

DSSS: étalement de spectre en séquence directe
FHSS : étalement de spectre avec sauts de fréquence

- La couche Liaison de données
  couche LLC et couche MAC

Cette norme permet d'avoir un débit de 1 ou 2Mb/s et elle utilise un accès au médium par compétition (méthode CSMA/CA)
(CA : Collision Avoidance)

Mais, évolution de cette norme Wi-Fi
(Wireless Fidelity)

Wi-Fi

Nom de la norme	Nom	Description
802.11a	Wi-fi	Débit : 54Mb/s, 8 canaux radio dans la bande de fréquence des 5 Ghz.
802.11b	Wi-fi	Débit : 11Mb/s, portée 300m, 3 canaux radio dans la bande de fréquence des 2,4 Ghz
802.11c	Pontage	Etablissement d'un pont pour la norme 802.11d
802.11d	International	Etablit les règles à respecter entre les différents pays pour transporter les données 802.11
802.11f	Roaming	Interopérabilité entre les différents points d'accès pour permettre l'itinérance (définition de l'IAPP)
802.11g	Wi-fi	Débit : 54MB/s, portée 300m, compatible avec 802.11b
802.11i	WPA2	Amélioration de la sécurité pour les normes a, b et g.
802.11n	Wi-fi 4	Débit : 600 Mb/s avec intégration de la norme i mais pas de compatibilité avec les normes précédentes
802.11ac	Wi-fi 5	Débit :1 300 Mb/s , utilisation de la bande de fréquences des 5 Ghz
802.11ax	Wi-fi 6	Débit max :10 Gb/s , utilisation de la bande de fréquences de 1 à 7,1 Ghz, QAM à 1024
802.11be	Wi-fi 7	A venir… 46 Gb/s, QAM à 4096, multi bande

Topologies sans fils (1)

- **2 Sortes d'équipement**
  - *Une station sans fil*
    - un ordinateur, smartphone, etc muni d'une carte Wifi

      (carte PCI, PCMCIA, adaptateur USB, carte compactflash, …)
  - *Un point d'accès* (Access Point) ou borne sans fil
    - joue le rôle de pont entre réseau filaire et sans fil
    - équipé : d'un émetteur/récepteur radio
      d'une carte réseau filaire
      d'un logiciel de pontage conforme à la norme 802.11d

Access Point

Topologies sans fils (2)

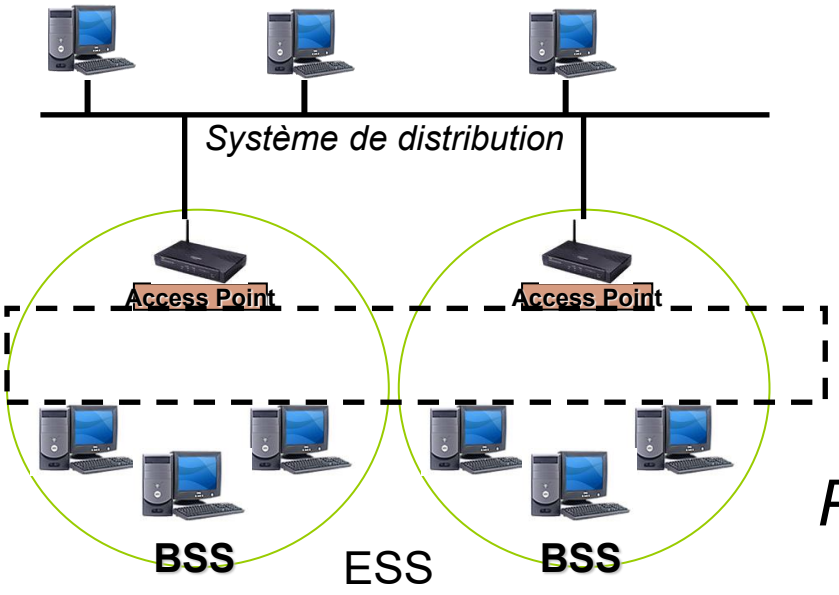
➢ Mode Infrastructure, autrement nommé HOTSPOT

• Au minimum , 1 AP + postes sans fil

BSS : Basic Service Set

- identifié par un BSSID (abrégé en SSID -> Service Set Identifier)

Toute communication passe par le Point d'Accès



• Plusieurs BSS forment un ESS (Extended Service Set) relié par un DS (Système de Distribution)

- identifié par un SSID

Possibilité de roaming si même SSID

Topologies sans fils (3)

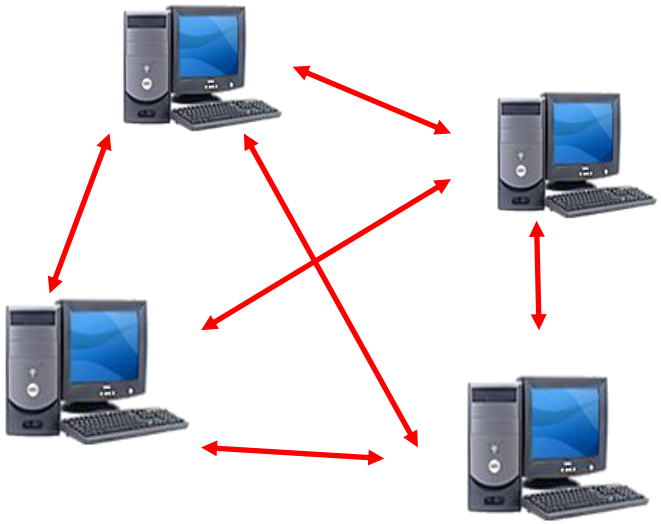
➢Mode Ad-Hoc

• Aucun AP, que des postes sans fil

IBSS : Independant Basic Service Set

- identifié par un SSID

Communication directe entre poste



• Problème pour le routage

si A ---> B
si B ---> C } alors A ~~--~~> C

Tout le monde doit voir tout le monde
ou
Pc configuré comme routeur

Trames utilisées

❑La couche MAC

- Similaire à la couche Mac ethernet pour les adresses
- ***Fonctionnalité***
  - Contrôle d'accès au support
  - Contrôle d'erreur par CRC
  - Fragmentation et réassemblage
  - Gestion de l'énergie
  - Gestion de la mobilité
- ***Deux méthodes d'accès pour le 802.11a, b, g, n, ac,…***
  - **DCF** (Distributed Coordination Function) : utilisation pour les données asynchrones, collisions possibles
  - **PCF** (Point Coordination Function) : utilisation pour les données synchrones, pas de collision (méthode non utilisée).

Distributed Coordination Function

❖DCF

- **Basé sur un accès CSMA/CA**

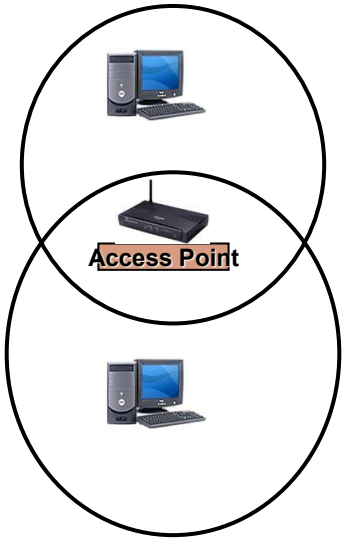
Pour émettre :

- On écoute le support (ondes)
- Si libre pendant un temps donné (*DIFS*, Distributed Inter Frame Space)
  -> transmission d'une trame Ready To Send (RTS) contenant les informations sur le volume de données et la vitesse de transmission.
  -> réception d'un Clear To Send (CTS)
  -> envoie des données
  -> récupération d'un ACK pour chaque trame

(RTS et CTS sont maintenant optionnelles)

Pourquoi un ACK pour chaque trame ?

2 stations peuvent vouloir émettre en même temps sans se voir. (Collision Avoidance…)



Les Trames WiFi

Couche MAC pour les trames de données

Contrôle de trame 2 octets	Durée/ID 2 octets	Adresse 1 6 octets	Adresse 2 6 octets	Adresse 3 6 octets	Séquence 2 octets	Adresse 4 6 octets

Corps de la trame 0 à 2312 octets	CRC 4 octets

Contrôle de trame

Version de protocole (2 bits)	Type (2 bits)	Sous-Type (4 bits)	To DS (1 bit)	From DS (1 bit)	More Frag (1 bit)	Retry (1 bit)	Power Mgt (1 bit)	More Data (1 bit)	WEP (1 bit)	Order (1 bit)

Version : actuellement, 00
Type : 3 types, plusieurs sous-types (00 : gestion, 01:contrôle, 10 : données)
To DS ou From DS : trame vers ou en provenance du système de distribution
More fragment : 1, trame fragmentée et pas dernier fragment, 0 sinon
Retry : 1 , retransmission
Power management : 1 , économie d'énergie, 0 actif
More Data : 1 si d'autres données à faire parvenir à la station
WEP : trame chiffrée par WEP ou non
order : Trame ordonnée ou non

Sécurité Wifi (1)

Problème : impossible d'arrêter les ondes

-> chiffrement des données sur le médium (niveau 2)

-> gérer par la norme : **WEP**

- Implémentation WEP (Wired Equivalent Privacy) (clé sur 40 bits / 104bits) donnée par les utilisateurs auquel est rajouté un vecteur d'initialisation (24 bits).

Fonctionnement : chiffrement RC4 en utilisant clé + vecteurs d'initialisation (IV)

message envoyé = (M.c(M)) xor RC4(IV . K)

c(M) = cheksum de M et K = clé

le RC4 donne des séquences pseudo-aléatoires

Le vecteur d'initialisation change à chaque trame envoyée, on lui rajoute 1

(assez facilement crackable du fait de RC4 et du vecteur d'initialisation

Actuellement, quelques dizaines de minutes pour cracker clé WEP

WEP ne doit plus être utilisé….

Sécurité Wifi (2)

- **Evolution**
  - Utilisation de la norme WPA (Wifi Protected Access)
    - remplacement de la clé WEP par TKIP (Temporal Key Integrity Protocol)
    - clé sur 256 bits
    - même algorithme que WEP
  - Utilisation de la norme WPA2, et WPA3
    - clé sur 2048 bits si nécessaire
    - chiffrement par AES
    - nouvel algorithme pour chiffrer les datas
  - Norme 802.1x

    => concerne spécifiquement l'authentification

    - 3 acteurs : -> le client (demandeur ou supplicant)
      -> le point d'accès relais (NAS : Network Access Server)
      -> le serveur d'authentification = serveur RADIUS

    codage en utilisant les trames EAP : Extensible Authentication Protocol

La couche LLC

- Les fonctions de la couche 2 non prises en charge par la couche MAC ont été placées dans la sous-couche LLC (Logical Link Control) :
  - points d'accès pour les entités des fournisseurs de couches 3.
  - rattrapage des erreurs (transformées en pertes par les couches MAC).
  - contrôle de flux.

Mais comme les 2 dernières fonctions ne sont pas toujours nécessaires, différentes couches LLC ont été spécifiées

Ethernet n'utilise pas de couche LLC, Wifi l'utilise.