Cours réseaux: MAC IEEE 802.11

Kamal Mehaoued

Département d'informatique, Université de Béjaia

2022/2023

Plan du cours

Couche MAC

La couche MAC de 802.11 peut utiliser deux modes de fonctionnement :

Distributed Coordination Function DCF

est un mode qui peut être utilisé par tous les mobiles, et qui permet un accès équitable au canal radio sans aucune centralisation de la gestion de l'accès (mode totalement distribué). Ce mode peut aussi bien être utilisé en mode ad hoc qu'en mode infrastructure.

Point Coordination Function

est un mode dans lequel les stations de base ont la charge de la gestion de l'accès au canal dans leur zone de couverture pour les mobiles qui leur sont rattachés.

Couche MAC

Dans les réseaux ad hoc multi-sauts, il n'y a pas de stations de base fixes et c'est donc le mode DCF qui sera employé.

Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)

La première caractéristique de la couche MAC de 802.11 est donc d'utiliser des acquittements pour détecter ces collisions et permettre la retransmission des paquets qui ont été perdus

Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)

en l'absence d'acquittement, l'émetteur sait qu'il doit retransmettre.

Couche MAC

Il faut noter que 802.11 peut envoyer une trame à un récepteur spécifique (unicast) ou la diffuser (broadcast). Dans le cas de la diffusion, il n'y a pas d'acquittement et des paquets peuvent être perdus de manière tout à fait silencieuse

Couche MAC

L'idée retenue pour 802.11 est donc :

- Lorsque le canal devient libre, attendre une période de durée aléatoire supplémentaire appelée backoff avant d'émettre.
- Ce mécanisme s'applique lorsque le canal devient libre aussi bien après une de nos propres émissions qu'après toute autre émission
- Ainsi, si plusieurs mobiles veulent émettre, il y a peu de chances pour qu'ils aient choisi la même durée.
- Celui qui a choisi le plus petit backoff va commencer à émettre, et les autres vont alors se rendre compte qu'il y a à nouveau de l'activité sur le canal et vont attendre.
- La figure ci-dessous schématise ce qui se passe lorsque deux mobiles à portée de communication veulent émettre vers un troisième et que le canal devient libre. le mobile 1 prends 3 le mobile 2 prends 5

Couche MAC

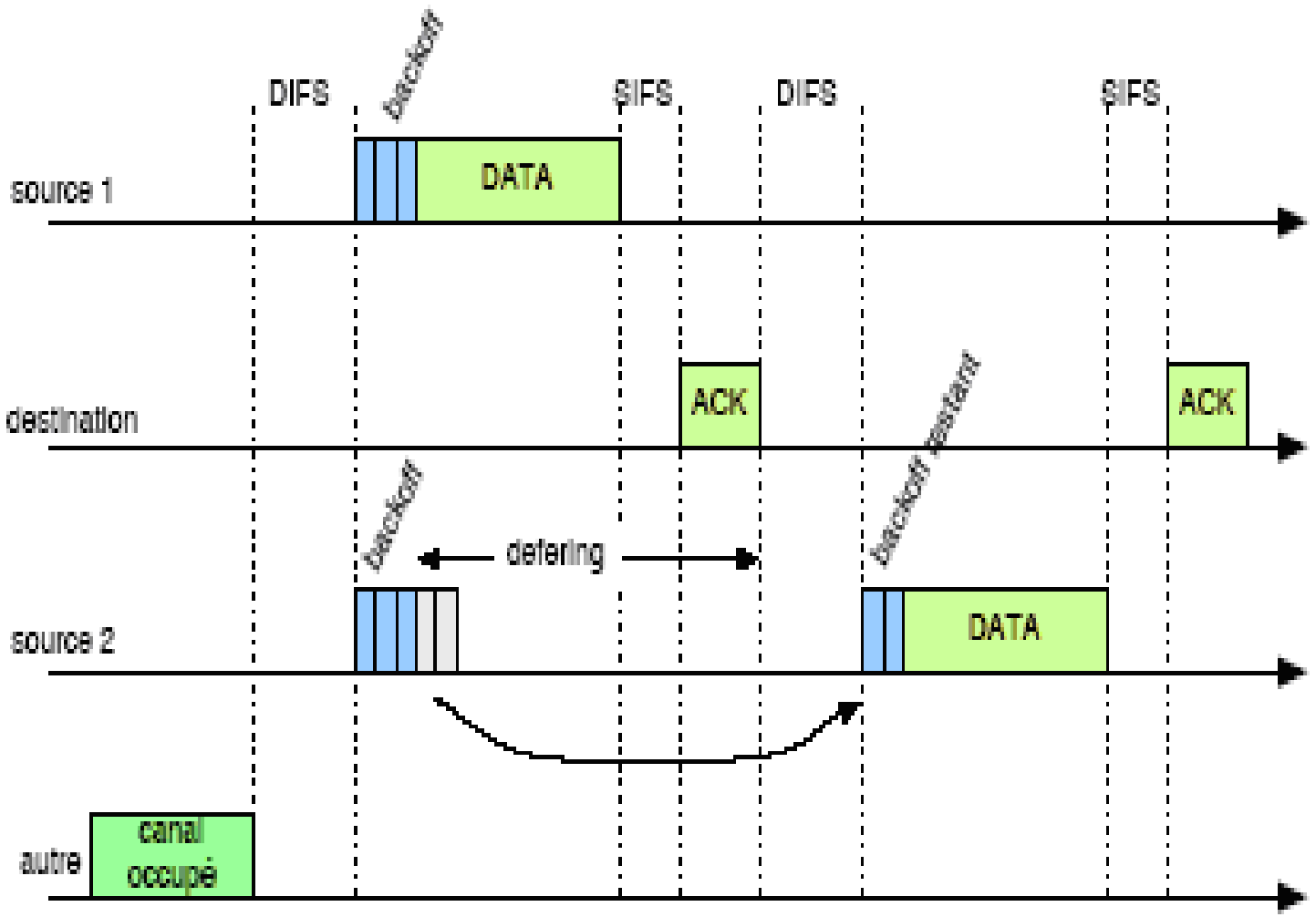

Figure – Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)

Le mécanisme du backoff

- Lorsque le canal devient libre, avant toute chose, il faut qu'il le reste pour une période DIFS
- Si le canal est resté libre durant toute cette période, alors les mobiles qui veulent émettre choisissent un backoff aléatoire exprimé en un nombre de time slots d'une durée fixe de 20 micro secondes
- Le backoff est choisi au hasard dans un intervalle appelé Contention Window (CW)
- Dans l'exemple précédent le mobile 1 a tiré 3 et le mobile 2 a tiré 5

Le mécanisme du backoff

- Une fois ce tirage effectué, tant que le canal reste libre, les mobiles décrémentent leur backoff
- Dès que l'un d'eux a terminé (ici le mobile 1), il émet
- L'autre mobile, dès qu'il détecte le regain d'activité sur le canal stoppe la décrémentation de son backoff et entre en période de defering.
- Il faut noter que le temps de pause qui sépare un paquet de données de son acquittement est appelé SIFS (Short Inter-Frame Space)
- le SIFS qu'il est plus court que DIFS

Le mécanisme du backoff

- Lorsque les données du mobile 1 ont été acquittées et que DIFS s'est écoulé sans activité sur le canal
- e mobile 2 peut reprendre la décrémentation de son backoff.
- Comme aucun autre mobile ne vient l'empêcher de terminer et il peut donc finalement envoyer ses données.
- Le mécanisme de backoff limite les risques de collision mais ne les supprime pas complètement.
- Aussi, si une collision se produit quand même (détectée grâce à l'absence d'acquittement), un nouveau backoff va être tiré au hasard.
- Mais à chaque collision consécutive, la taille de la fenêtre va doubler afin de diminuer les chances que de telles collisions se répètent.

Le mécanisme RTS/CTS

- Afin de remédier aux problèmes du nœud caché et/ou du nœud exposé 802.11 propose le mécanisme rts/cts
- Ce mécanisme propose l'utilisation des paquets de contrôle appelés Request To Send (RTS) et Clear To Send (CTS)
- Un mobile qui veut émettre ne va plus directement envoyer son gros paquet de données, mais plutôt un petit paquet RTS pour lequel les chances de collision sont plus faibles.
- A ce paquet RTS, le destinataire va répondre par un petit paquet CTS qu'il diffuse à tout son voisinage
- Au niveau des mobiles, la réservation du canal est implémentée grâce au Network Allocation Vector (NAV).
- Dans chaque nœud, le NAV indique pour combien de temps le canal est utilisé par un autre nœud

Le mécanisme RTS/CTS

- Les paquets RTS et CTS contiennent des informations qui permettent de réserver le canal pour la durée de transmission des données qui vont suivre
- Un mobile qui reçoit un CTS alors qu'il n'a pas envoyé (ni même détecté de RTS) sait que quelqu'un d'autre va émettre et doit donc attendre.
- Le mobile qui a envoyé le RTS sait, quand il reçoit le CTS correspondant, que le canal a été réservé pour lui et qu'il peut émettre.

Le mécanisme RTS/CTS

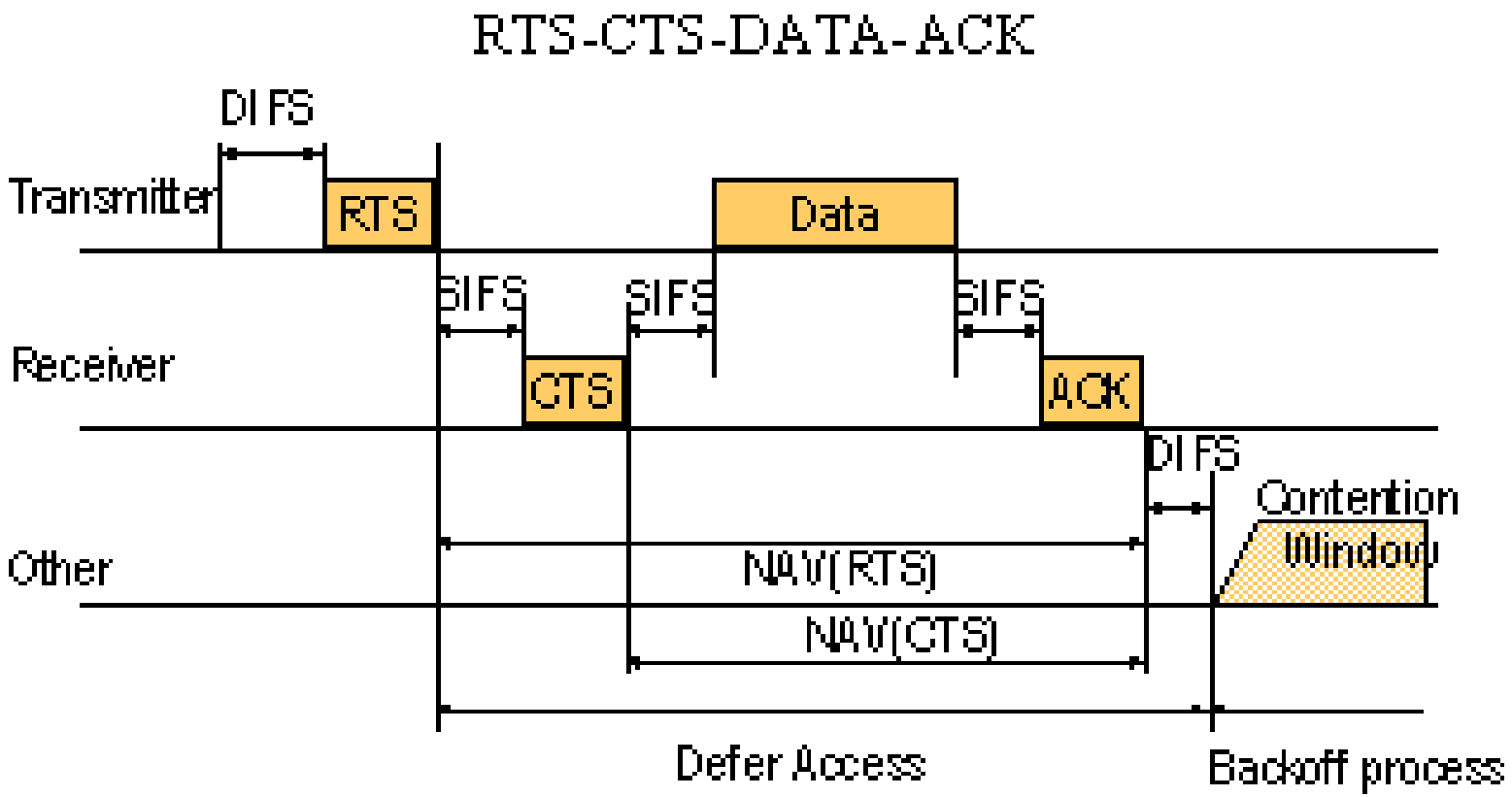

Figure – Le mécanisme RTS/CTS

Extended Inter Frame Space EIFS

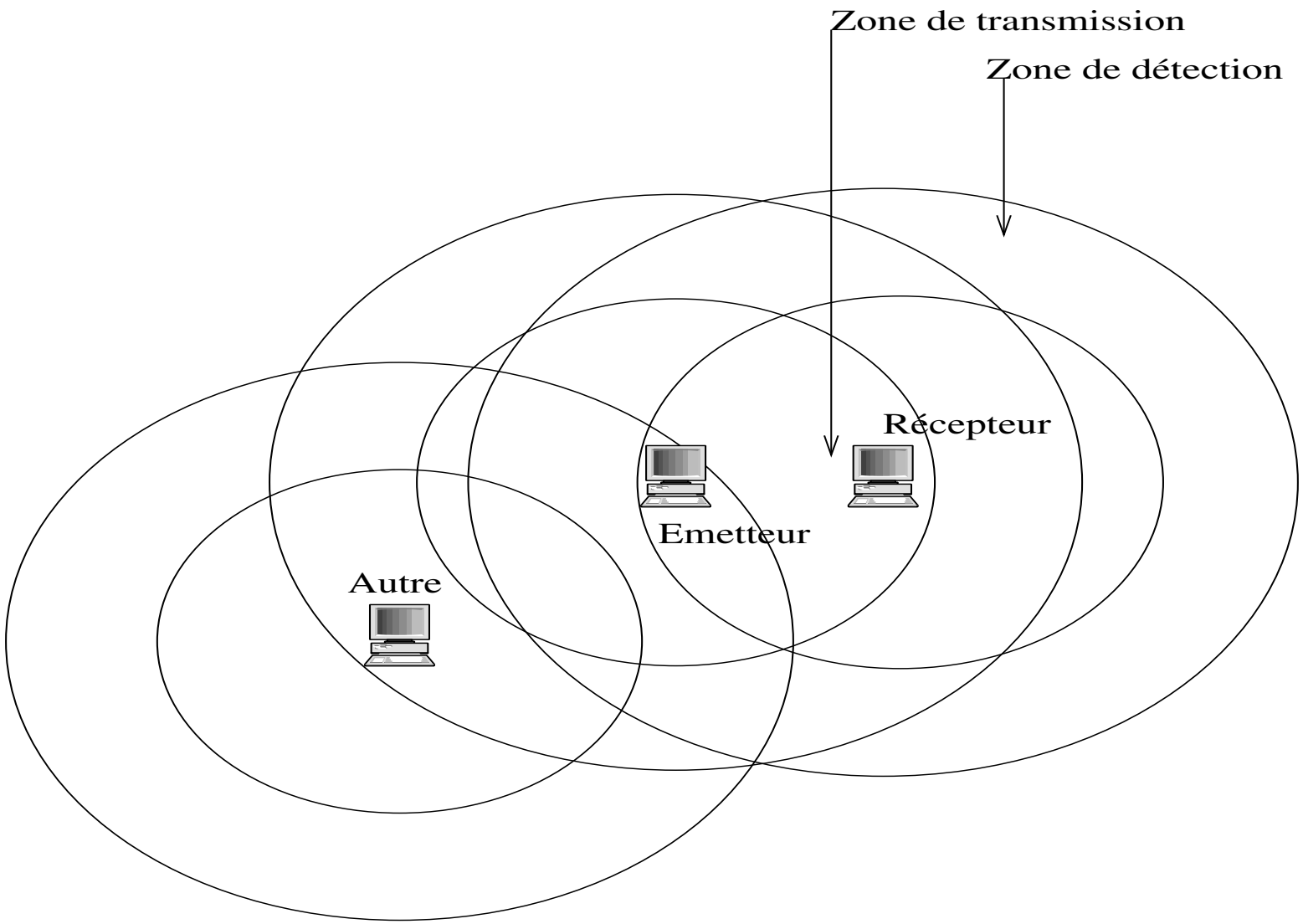

Figure – Extended Inter Frame Space

Extended Inter Frame Space EIFS

le nœud de gauche ("autre") détecte la porteuse de l'activité sans pour autant comprendre ses messages (le signal est trop faible pour être décodé, mais suffisamment fort pour être reconnu comme)

Les paquets envoyés par le récepteur ne sont quant à eux pas détectés du tout par le mobile de gauche (autre)

Dans cette situation, 802.11 impose l'utilisation d'un Extended Inter Frame Spacing(EIFS), afin d'éviter une collision au niveau de l'émetteur au moment du CTS et de l'acquittement par le récepteur

Extended Inter Frame Space EIFS

L'émetteur envoie tout d'abord un paquet de contrôle RTS.

Ce paquet est reçu par le récepteur, qui va y répondre par un CTS.

Le mobile de gauche, lui, a détecté de l'activité au moment du RTS mais sans comprendre le paquet

Le mécanisme de defering présenté précédemment l'empêche d'émettre pendant l'envoi du RTS (canal occupé) et pendant une période DIFS consécutive (on est toujours obligé d'attendre que le canal soit libre pendant DIFS pour émettre)

Mais DIFS est plus court que SIFS+CTS.

Extended Inter Frame Space EIFS

Si jamais le mobile de gauche avait terminé de décrémenter son backoff trop vite, il aurait pu émettre pendant le CTS causant une collision au niveau de l'émetteur.

Pour protéger le CTS (et de manière similaire l'acquittement), 802.11 impose qu'un nœud doive attendre pendant un temps EIFS lorsque le canal redevient libre mais que le paquet n'a pas été compris

la longueur de EIFS étant suffisante pour que l'envoi du CTS ou de l'ACK se déroule dans de bonnes conditions.

HiperLAN 1

High Performance Local Area Network type 1 (HiperLan 1) est un standard de l'European Technical Standard Institute (ETSI)

Il décrit le fonctionnement d'équipements travaillant dans la bande des 5.15-5.30 GHz et permettant d'atteindre des débits de 23.5 Mbit/s sur une distance d'environ 50 mètres.

L'architecture est totalement décentralisée.

Il n'y a pas de notion de point d'accès mais les nœuds HiperLAN 1 peuvent cependant avoir des rôles de passerelles.

HiperLAN 1

le mécanisme d'accès au médium EY-NPMA (Elimination Yield-Non Preemptive Multiple Access) est au cœur du système

Le fonctionnement de EY-NPMA est particulièrement intéressant et il est prévu pour fonctionner dans un contexte ad hoc

Il fonctionne en trois phases :

1. la phase de priorité.
2. La phase d'élimination.
3. La phase d'écoute.

La phase de priorité.

Cinq niveaux de priorité sont définis par la norme (de 0 pour le plus prioritaire à 4) et la phase de priorité est donc divisée en cinq slots.

Au début d'un nouveau cycle de transmission, tous les nœuds qui veulent accéder au canal vont envoyer un burst de signalement, dont la date de début dépend de la priorité du paquet

Plus la priorité est élevée, plus le burst commence tôt.

Si l'on détecte de l'activité avant d'avoir pu émettre, c'est que quelqu'un plus prioritaire a déjà accès

La phase d'élimination

Il se peut que plusieurs nœuds veuillent émettre en même temps des paquets de priorités identiques.

Dans ce cas, chaque nœud va poursuivre l'envoi de son burst de signalement pendant un nombre aléatoire de slots.

Ce sera celui qui aura tiré le plus grand nombre qui l'emportera

Dès que l'émission de notre burst est terminée, nous écoutons le canal

Si nous y détectons de l'activité, c'est qu'un autre nœud a tiré un plus grand nombre que nous, et nous abandonnons pour ce cycle

La phase d'écoute

S'il reste plusieurs nœuds en lice alors l'élimination va se terminer dans la cette phase.

Un nombre aléatoire de slots est choisit.

C'est celui qui aura tiré le plus petit qui pourra transmettre.

Chaque nœud attend pendant la durée qu'il a déterminé, en écoutant le canal.

Si il détecte de l'activité alors qu'il n'a pas fini d'attendre, il sait que quelqu'un a tiré un plus petit nombre que lui et n'émettra pas durant ce cycle.

A la fin de l'attente si le canal est toujours libre, alors il émet

Exemple

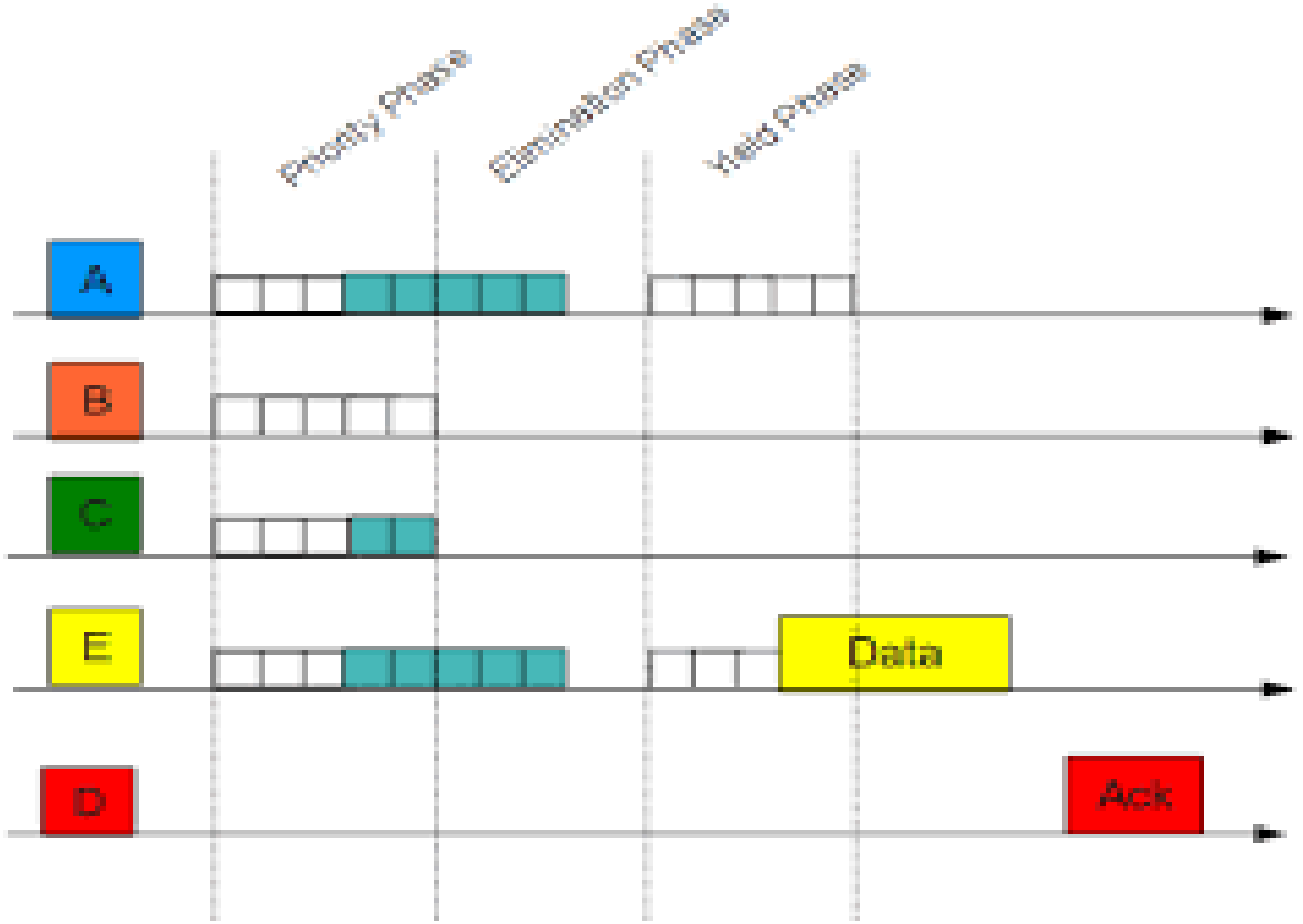

Figure – Exeple HyperLAN 1

HiperLAN 2

HiperLAN type 2 est très différent dans son architecture d'HiperLAN type 1.

Contrairement au type 1, le type 2 est basé sur une centralisation poussée

Les points d'accès sont d'ailleurs indifféremment appelés Access Points (AP) ou Central Controler (CC).

Les points d'accès sont reliés entre eux par une infrastructure réseau filaire ou non-filaire