

Réseaux et Systèmes (MIN 15112)

2025 - 2026

Zhiyi Zhang

zhiyi.zhang@uvsq.fr

<https://www.zhiyizhang.com>

Annoncement

Contrôle continu

Mercredi 12/11/2025

11h20 – 12h50

Amphi B - Descartes

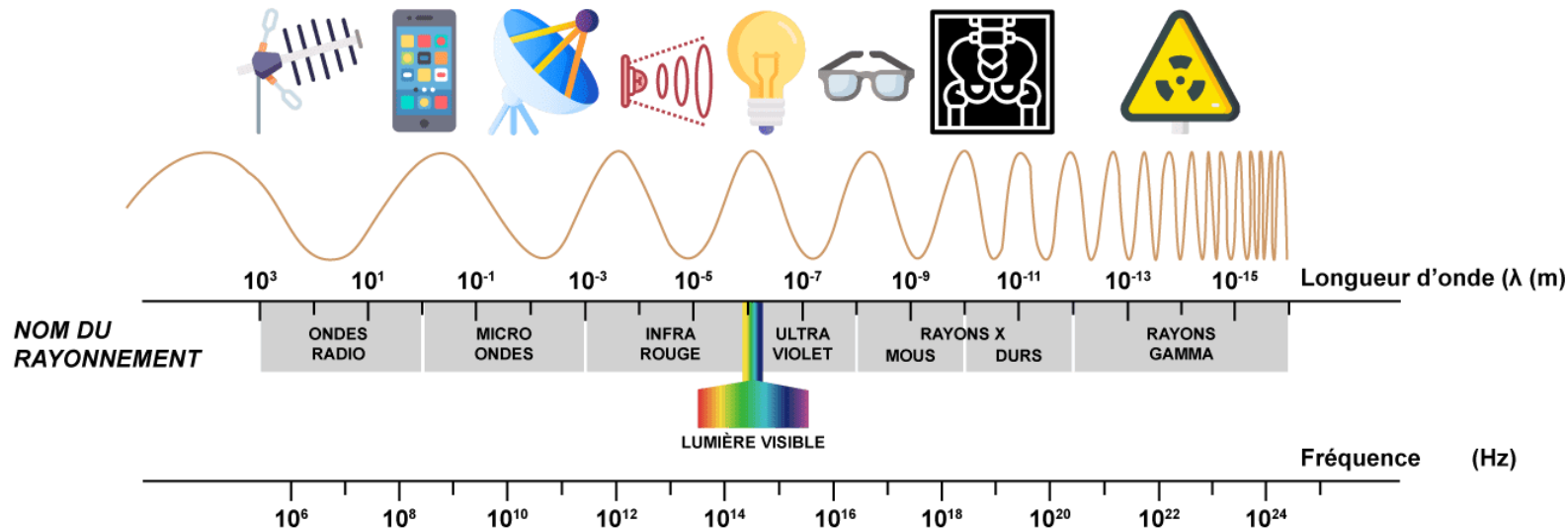
Document interdit

Calculatrice autorisée

WiFi & CSMA/CA

Notions de base

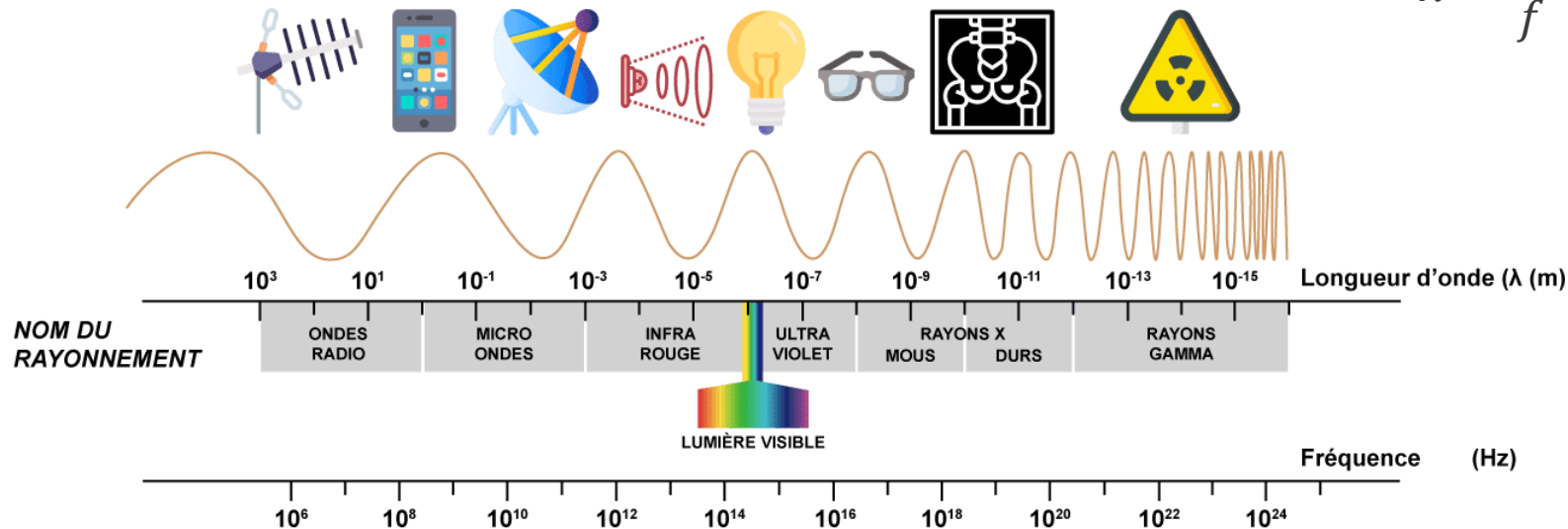
Spectre des ondes électromagnétiques



Notions de base

Spectre des ondes électromagnétiques

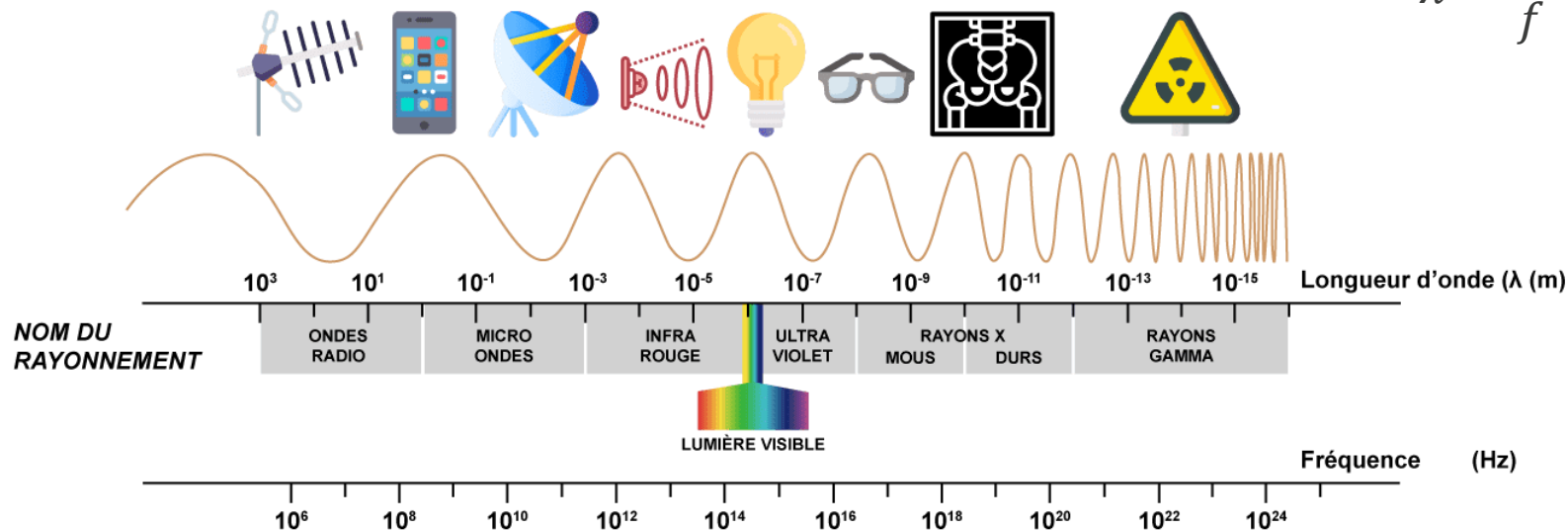
$$\lambda = \frac{c}{f}$$



Où se déroule la communication sans fil ?

Spectre des ondes électromagnétiques

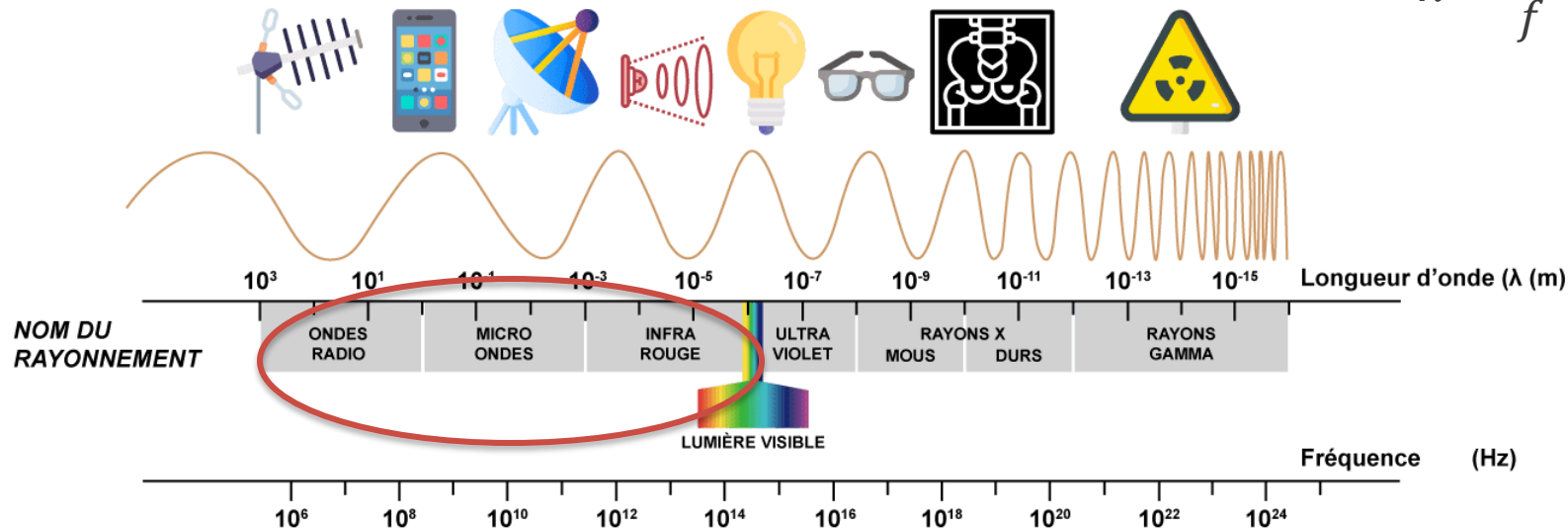
$$\lambda = \frac{c}{f}$$



Notions de base

Spectre des ondes électromagnétiques

$$\lambda = \frac{c}{f}$$



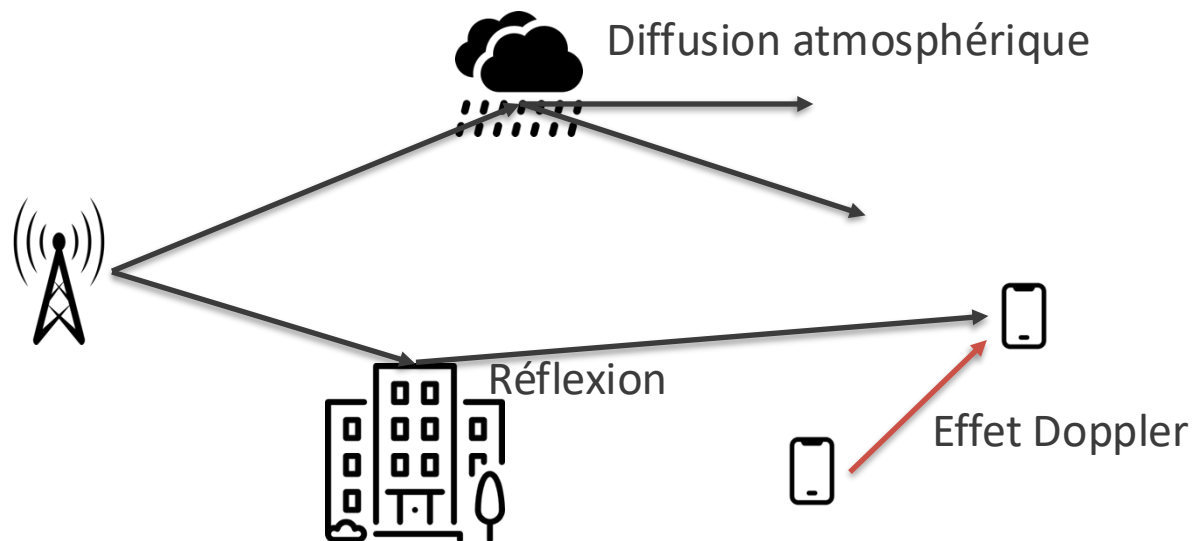
Classification

Nom de la bande	f	λ
Low Frequency	30 kHz – 300 kHz	10 km – 1 km
Medium Frequency	300 kHz – 3 MHz	1 km – 100m
High Frequency	3 MHz – 30 MHz	100 m – 10 m
Very High Frequency	30 MHz – 300 MHz	10 m – 1 m
Ultra High Frequency	300 MHz – 3 GHz	1 m – 10 cm
Super High Frequency	3 GHz – 30 GHz	10 cm – 1 cm
Extremely High Frequency	30 GHz – 300 GHz	1 cm – 1 mm
Infrared	300 GHz – 400 THz	1 mm – 700 nm

Applications

Nom de la bande	Utilisation
Low Frequency	Navigation aéronautique et maritime, météorologie
Medium Frequency	Radio AM
High Frequency	Communications maritimes, aéronautiques et militaires
Very High Frequency	Radio FM, télévision analogique, communications aéronautiques
Ultra High Frequency	Télévision terrestre (numérique), réseaux cellulaires, WiFi, GPS
Super High Frequency	WiFi, télévision par satellite
Extremely High Frequency	Radar, communication par satellite, 5G mmWave
Infrared	Télécommandes, lasers, LED, détection thermique

Propagation



Propagation

Free Space Path Loss (Perte de propagation en espace libre)

$$PL = \left(\frac{4 \pi d f}{c}\right)^2$$

$$PL \text{ (dB)} = 20 \log_{10} \left(\frac{4 \pi d f}{c}\right)$$

d : distance entre l'émetteur et le récepteur

f : fréquence du signal

c : vitesse de la lumière

Free Space Path Loss (Perte de propagation en espace libre)

$$PL = \left(\frac{4 \pi d f}{c}\right)^2$$

$$PL \text{ (dB)} = 20 \log_{10} \left(\frac{4 \pi d f}{c}\right)$$

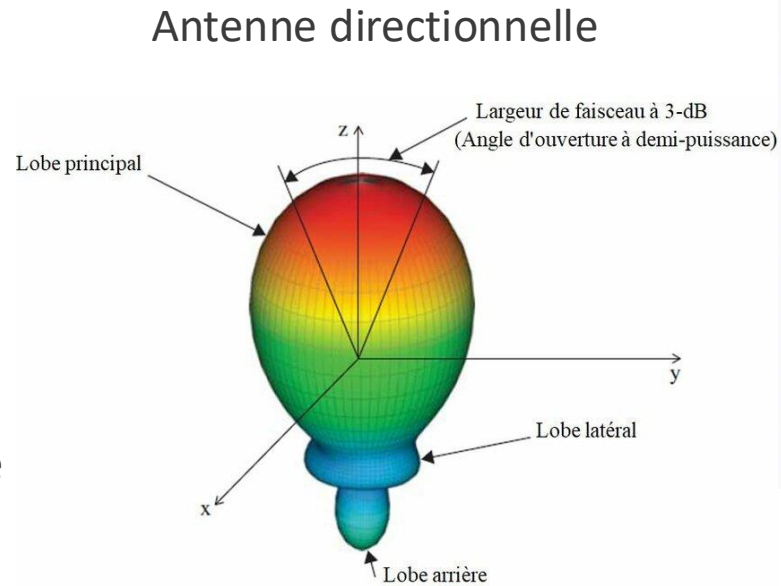
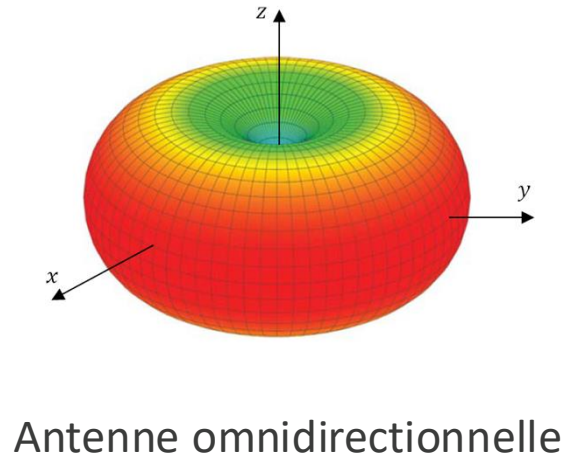
Plus la fréquence du signal est élevée,
Plus la distance est grande,
Plus la perte de signal est importante.

d : distance entre l'émetteur et le récepteur

f : fréquence du signal

c : vitesse de la lumière

Gain d'antenne



Bilan de liaison : permet de savoir si le signal reçu est suffisant pour décoder les données.

$$P_r \text{ (dBm)} = P_t \text{ (dBm)} + G_t \text{ (dBi)} + G_r \text{ (dBi)} - PL \text{ (dB)} - L_{\text{autres}} \text{ (dB)}$$

P_r : Puissance reçue

P_t : Puissance transmise

G_t : Gain de l'antenne émettrice

G_r : Gain de l'antenne réceptrice

PL : Atténuation de propagation

L_{autres} : Pertes diverses (connecteur, câble...)

Capacité du canal : débit théorique

$$C = B \log_2 (1 + \text{SNR})$$

Plus le signal est fort,
plus la bande passante est large,
plus le débit est élevé.

B : bande passante du canal

SNR : rapport signal sur bruit ($10 \log_{10} \left(\frac{P_{\text{Signal}}}{P_{\text{Bruit}}} \right)$)

Rappel : CSMA

- Chaque station écoute le canal avant de transmettre
- Si le canal est occupé, la station attend, puis :
 - transmet dès qu'il devient libre (1-persistent)
 - choisit un temps d'attente aléatoire avant de réessayer (0-persistent)
 - transmet avec une probabilité de p lorsque le canal est libre (p -persistent)

Rappel : CSMA/CD

- CSMA : écouter avant de parler
- CD : écouter pendant la transmission
- Si le signal reçu \neq le signal envoyé \rightarrow collision détectée
- Envoyer un signal de brouillage
- Vérifier le nombre de tentative (limite de retransmission)
- Doubler la fenêtre de contention et back-off

CSMA & WiFi

CSMA/CD : collision détectable → retransmission ?

~~CSMA/CD : collision détectable → retransmission ?~~

Dans les réseaux sans fil, on ne peut pas détecter les collisions facilement.

- Les stations ne peuvent pas émettre et écouter en même temps
- L'atténuation du signal rend la détection de collision presque impossible

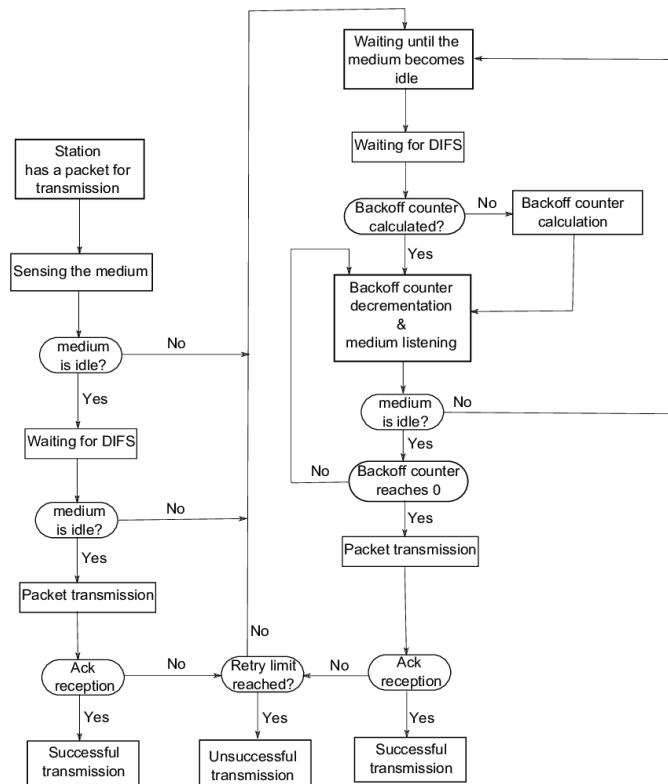
Donc, on utilise CSMA/CA (CSMA with Collision Avoidance)

- CSMA/CA est apparu dans les années 1980, initialement comme un protocole MAC utilisé dans le réseau Apple LocalTalk.
- Ensuite, il est devenu la base du standard IEEE 802.11 (WiFi).

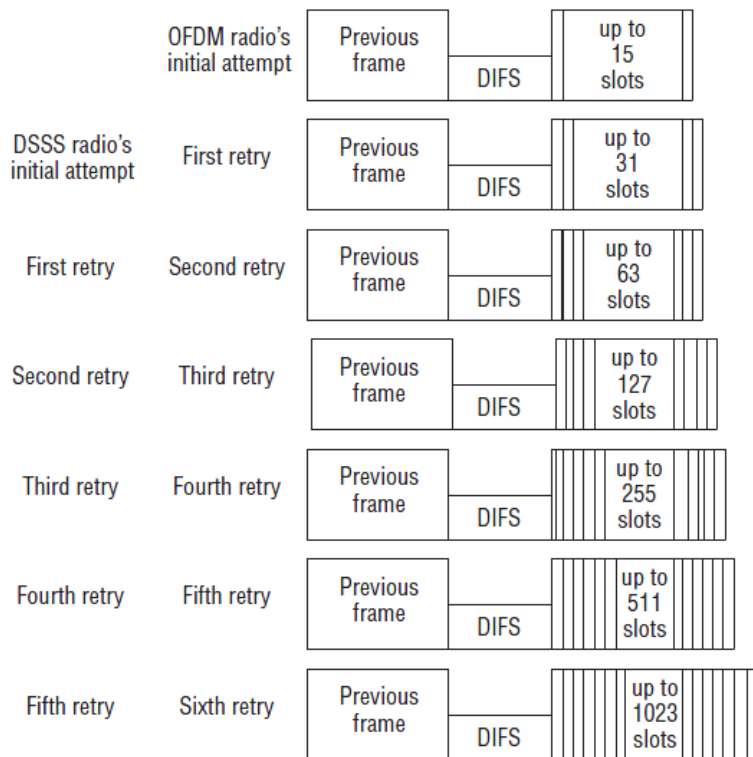
CSMA/CA

- La station écoute le canal (Carrier Sense)
- Si le canal est libre -> transmettre
- Si le canal est occupé -> back-off aléatoire
- Le temps d'attente est découpé en slots
- Si un slot est libre, le compteur de back-off est décrémenté
- Si un slot est occupé, le compteur est suspendu
- La station transmet lorsque le compteur atteint 0
- Si pas de ACK reçu, doubler la fenêtre de contention et recommence

CSMA/CA



CSMA/CA



En IEEE 802.11, 6 back-off (max) est autorisé.

Si la 7^{ème} transmission échoue encore, la trame est abandonnée.

CSMA/CA

On n'utilise pas CSMA/CD dans les réseaux sans fil
-> atténuation du signal rend la détection de collision impossible

Mais le Carrier Sense fonctionne bien ?

On n'utilise pas CSMA/CD dans les réseaux sans fil
-> atténuation du signal rend la détection de collision impossible

Mais le Carrier Sense fonctionne bien ?

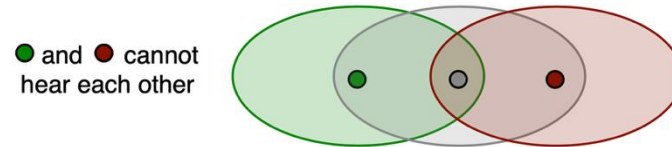
Pas toujours !

Problèmes des terminaux cachés

Terminaux cachés

Terminal caché : une station qui ne peut pas détecter une autre transmission en cours, car elle se trouve en dehors de la portée de l'émetteur. Mais leurs signaux peuvent entrer en collision au niveau du récepteur commun.

Terminal caché : une station qui ne peut pas détecter une autre transmission en cours, car elle se trouve en dehors de la portée de l'émetteur. Mais leurs signaux peuvent entrer en collision au niveau du récepteur commun.



Common scenarios

- sends DATA to ●
- wants to access the channel but hears the DATA from ●
- waits the end of DATA, then senses the channel idle and transmits
- collision between DATA and ACK

- sends DATA to ●
- wants to access the channel and senses it idle and transmits
- collision between DATA and DATA

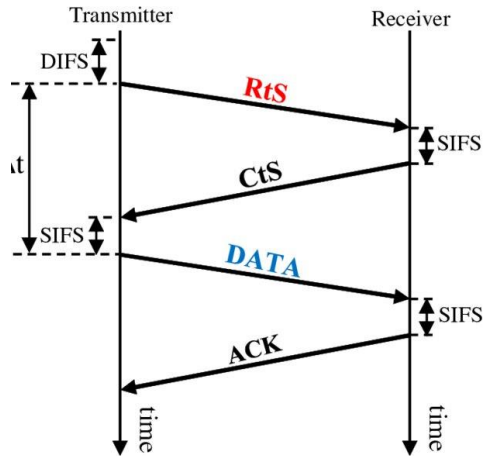
La probabilité de collision entre les terminaux cachés augmente avec la taille des messages

Deux messages de contrôle pour réserver le canal

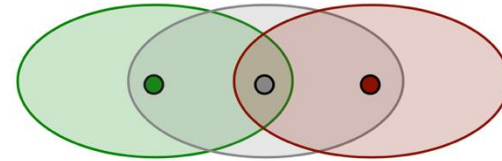
- RTS (Request-To-Send) : Demande d'autorisation d'émettre
- CTS (Clear-To-Send) : Autorisation d'émettre

RTS/CTS contiennent des informations sur la durée de la transmission suivante (DATA + ACK)

RTS/CTS



● and ● cannot hear each other



- sends RTS to ●
- sends CTS to ●
- hears the CTS and considers the channel busy for the announced duration
- sends DATA to ●
- sends ACK to ●

Le mécanisme RTS/CTS est également appelé détection virtuelle de porteuse (virtual carrier sense).

IEEE 802.11 : début

- En 1985, la US Federal Communications Commission a créé la **bande ISM** (Industrielle, scientifique et médicale) pour des utilisations **sans licence (2,4 GHz)**
- En 1990, IEEE a mis en place le comité 802.11
- En 1997, le standard IEEE 802.11 a été finalisé et il est devenu le standard pour les réseaux locaux sans fil (WLAN)

IEEE 802.11 : évolution

- Débit (théorique) plus élevé : 11 Mbps (b), 54 Mbps (g), 100+ Mbps (n), 500+ Mbps (ac), jusqu'à 10 Gbps (ax)
- Utilisation de différentes bandes de fréquences : 2,4 GHz; 5 GHz; 60 GHz
- Utilisation plusieurs antennes (MIMO) : n, ac, ax
- Intégration de la qualité de service (QoS) : e
- Environnements dédiés : réseaux maillés (s), communication véhiculaire (p)
- Améliorations de la sécurité : i, ax

IEEE 802.11 : version/génération

Wi-Fi generations

V.T.E

Gen. ^[3]	IEEE standard	Adopt.	Link rate (Mbit/s)	RF (GHz)		
				2.4	5	6
—	802.11	1997	1–2	✓		
—	802.11b	1999	1–11	✓		
—	802.11a	1999	6–54		✓	
—	802.11g	2003		✓		
Wi-Fi 4	802.11n	2009	6.5–600	✓	✓	
Wi-Fi 5	802.11ac	2013	6.5–6,933	^[a] ✓		
Wi-Fi 6	802.11ax	2021	0.4–9,608	✓	✓	
Wi-Fi 6E				✓	✓	✓
Wi-Fi 7	802.11be	2024	0.4–23,059	✓	✓	✓
Wi-Fi 8 ^[4]	802.11bn		0.4–23,059	✓	✓	✓

Historiquement, on utilise le nom des standards IEEE pour indiquer les versions de WiFi.
(b, g, n, ac, ax ...)

En 2018, la WiFi alliance a introduit une numérotation génération simplifiée afin d'identifier plus facilement les versions.

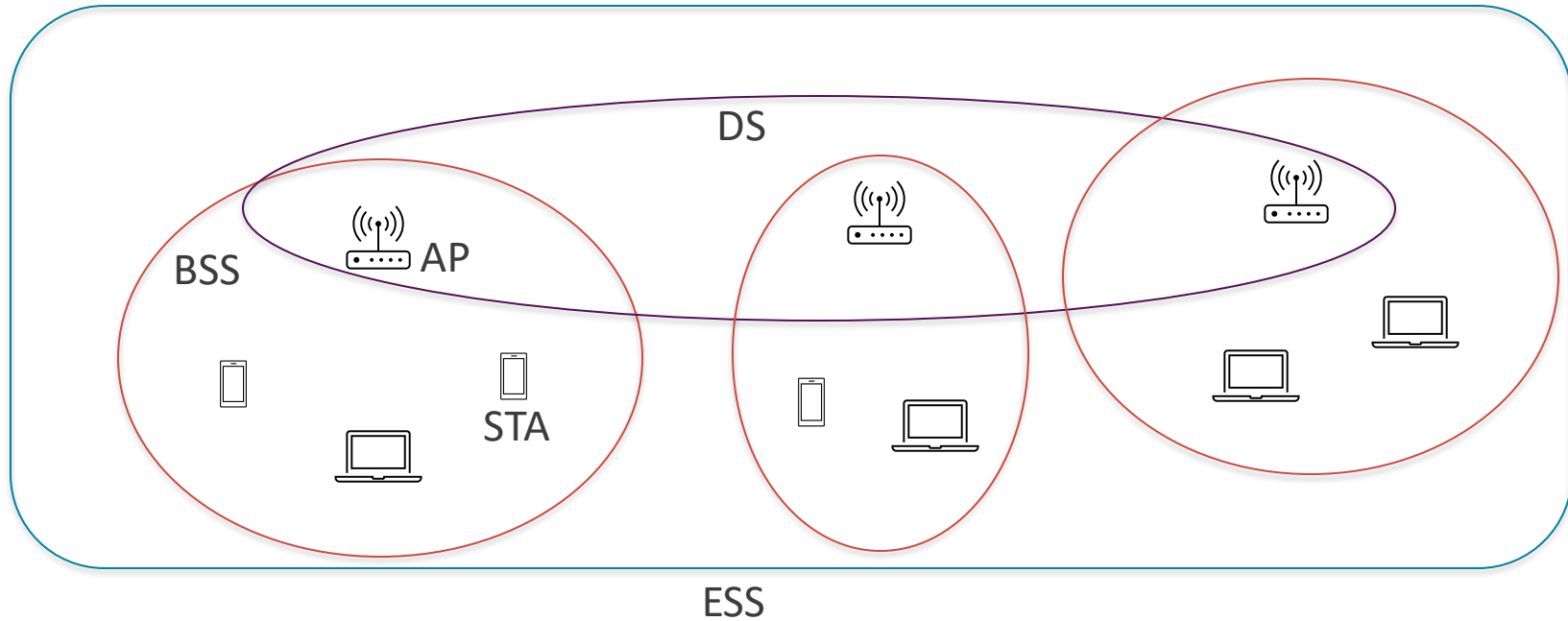


IEEE 802.11 : WiFi Direct

WiFi Direct : permet à deux ou plusieurs équipements WiFi de communiquer directement entre eux, sans passer par un point d'accès.

- Au moins un équipement compatible avec WiFi Direct
- L'un des équipements devient un point d'accès logiciel, appelé GO (Group Owner), auquel les autres (Group Client) se connectent directement
- Seul le GO est autorisé à connecter à un réseau externe

IEEE 802.11 : architecture



IEEE 802.11 : BSS

BSS (Basic Service Set)

BSS regroupe un ensemble de stations sans fil (STA) qui peuvent communiquer entre elles en suivant les mêmes règles d'accès au canal.

Avec ou sans point d'accès (AP)

Infrastructure BSS : AP + stations clientes. (classique, trafic passe toujours par l'AP)

Independent BSS (IBSS) : sans AP, les stations communiquent directement entre elles (mode ad hoc)

BSSID (BSS Identifier) : généralement, l'adresse MAC de l'AP

IEEE 802.11 : ESS

ESS (Extended Service Set)

Il est possible de relier plusieurs AP par un réseau appelée DS (Distribution System) afin de constituer un ESS.

Selon l'architecture, le DS peut être filaire ou sans fil.

ESSID (ESS Identifier) : nom du réseau WiFi visible par l'utilisateur (SSID)

ESSID est une chaîne de caractères.

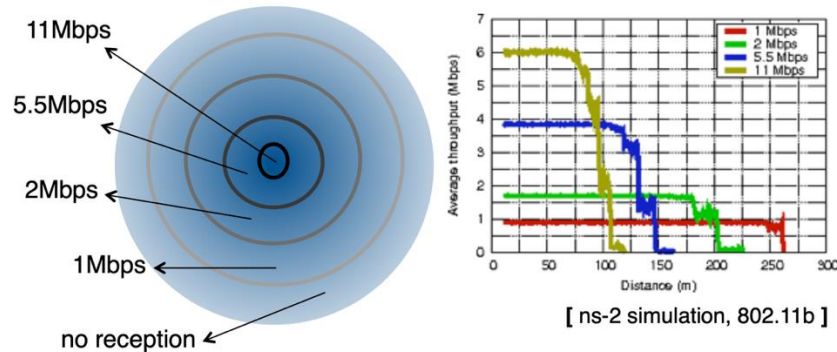
IEEE 802.11 : association

- **Scanning – la station recherche/choisit un AP**
 - **Passif** : la station attend simplement les trames de balise (beacon) envoyées périodiquement par les AP.
 - **Actif** : la station envoie des requêtes (probe request) pour solliciter une réponse des AP voisins.
- **Authentification – la station prouve qu'elle est autorisée à accéder au réseau**
 - **Ouverte** : accès libre
 - **Sécurisée** : AP envoie un défi (challenge), et la station doit répondre correctement à l'aide d'une clé partagée pour être authentifiée.
- **Association – la station entre dans le BSS**
 - La station envoie une requête d'association, puis l'AP répond
 - En cas de roaming, le nouvel AP informe l'ancien AP via le DS

IEEE 802.11 : modulation

La modulation détermine le débit.

- Pour décoder une modulation plus complexe, il faut un signal plus fort (meilleur rapport signal/bruit)
- Compromis entre le débit de transmission et la portée du signal



IEEE 802.11 : modulation

MCS (Modulation and Coding Scheme)

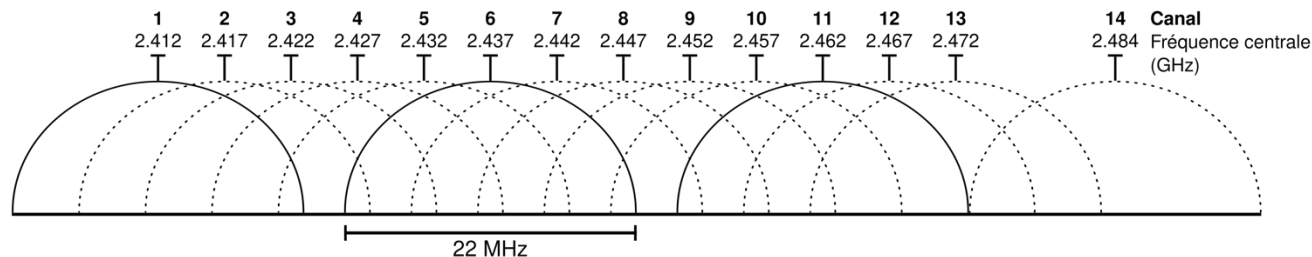
- Adaptation dynamique de la modulation et du taux de codage en fonction de l'état du canal
- Permet de faire varier dynamiquement le débit de données selon la qualité du signal
- <https://mcsindex.com/>

MCS	Modulation	Coding	40 MHz			
			Data Rate		Min. SNR	Min. RSSI
			800 ns	400 ns		
0	BPSK	1/2	13.5	15	5	-79
1	QPSK	1/2	27	30	8	-76
2	QPSK	3/4	40.5	45	12	-74
3	16-QAM	1/2	54	60	14	-71
4	16-QAM	3/4	81	90	18	-67
5	64-QAM	2/3	108	120	21	-63
6	64-QAM	3/4	121.5	135	23	-62
7	64-QAM	5/6	135	150	28	-61
8	256-QAM	3/4	162	180	32	-56
9	256-QAM	5/6	180	200	34	-54

IEEE 802.11 : canaux (2,4 GHz)

Plusieurs canaux, mais pas totalement indépendants

- Leurs bandes spectrales se chevauchent partiellement
- Les transmissions sur deux canaux proches peuvent se perturber mutuellement



IEEE 802.11 : puissance d'émission

Réglementation française (ARCEP)

- Puissance d'émission limitée (bande 2,4 GHz)
 - Intérieur : 100 mW
 - Extérieur : 100 mW
- Puissance d'émission limitée (bande 5 GHz)
 - Extérieur / Intérieur : 5470 – 5725 MHz : 500 mW – 1 W
 - Intérieur uniquement
 - 5150 – 5250 MHz : 200 mW
 - 5250 – 5350 MHz : 100 mW – 200 mW

CSMA/CA implementation : DCF (Distributed Coordination Function)

4 types d'IFS (InterFrame Space)

- SIFS (Short IFS) : utilisé pour séparer des transmissions appartenant au même dialogue (avant l'envoi CTS ou ACK)
- PIFS (Point Coordination IFS) : utilisé dans le mode PCF
- DIFS (Distributed IFS) : IFS standard, utilisé pour séparer les transmissions appartenant à des dialogues différents (avant de lancer le back-off)
- EIFS (Extended IFS) : utilisé par une station qui a reçu une trame erronée

CSMA/CA implementation : DCF (Distributed Coordination Function)

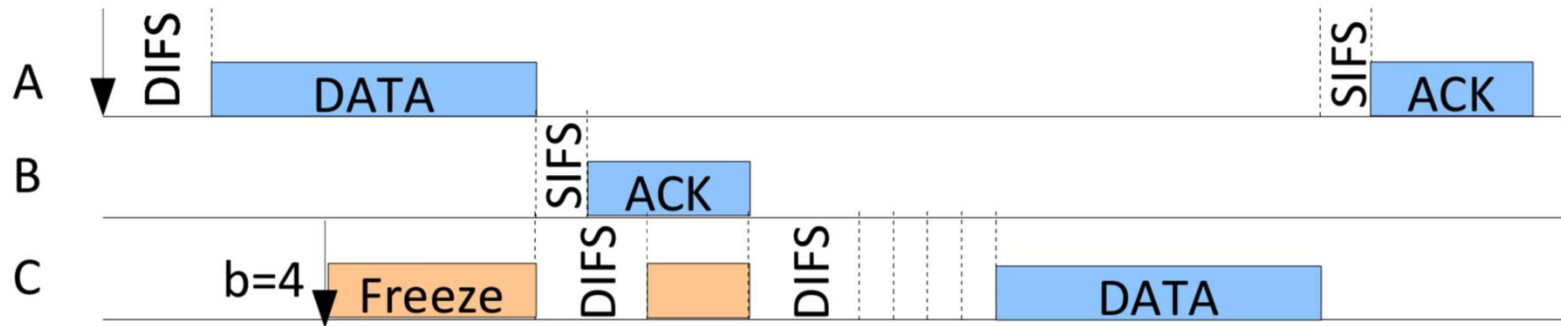
SIFS < PIFS < DIFS < EIFS

4 types d'IFS (InterFrame Space)

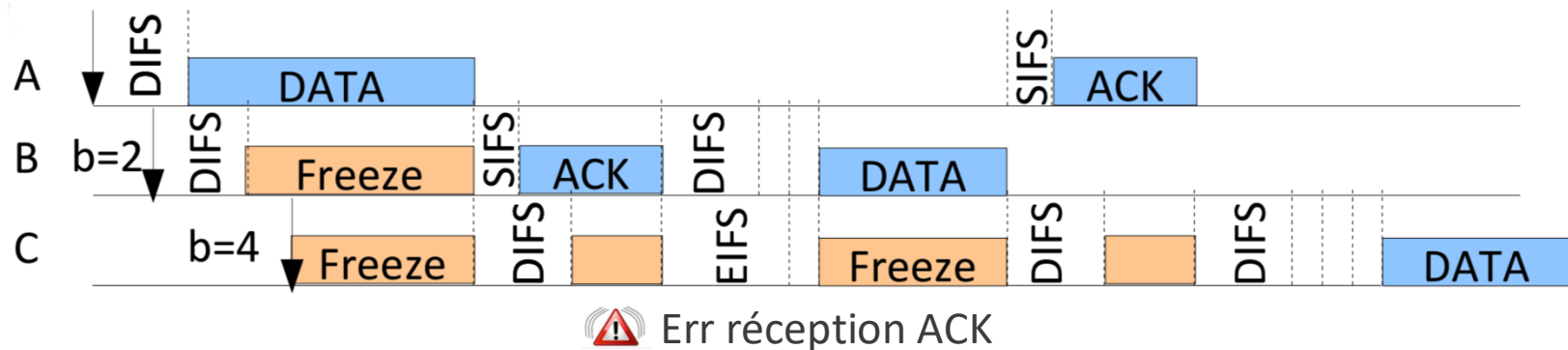
- SIFS (Short IFS) : utilisé pour séparer des transmissions appartenant au même dialogue (avant l'envoi CTS ou ACK)
- PIFS (Point Coordination IFS) : utilisé dans le mode PCF
- DIFS (Distributed IFS) : IFS standard, utilisé pour séparer les transmissions appartenant à des dialogues différents (avant de lancer le back-off)
- EIFS (Extended IFS) : utilisé par une station qui a reçu une trame erronée

IEEE 802.11 : DCF

Scénarios



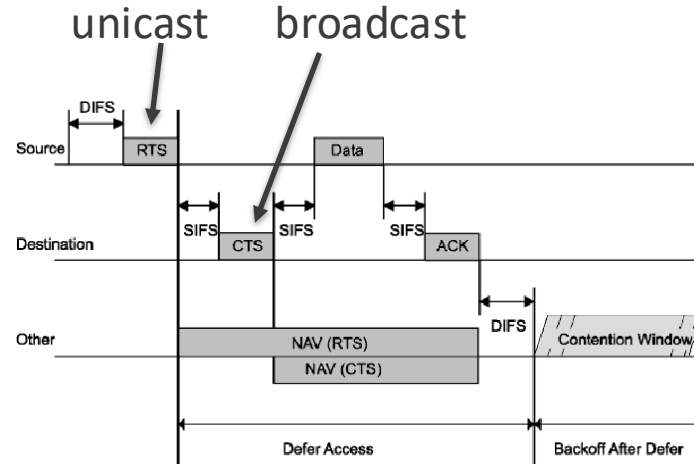
Scénarios



L'EIFS est appliqué par la DCF lorsque la couche PHY détecte une transmission, mais la trame n'est pas correcte (CRC failed)

IEEE 802.11 : DCF

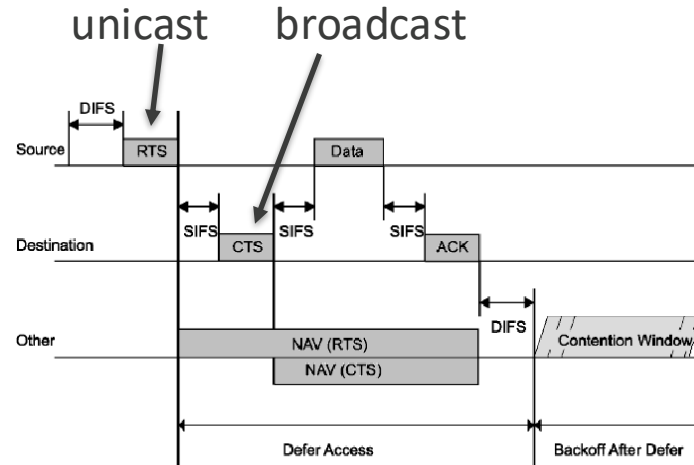
Scénarios



NAV (Network Allocation Vector) : Virtual Carrier Sense
Dans RTS, on a la durée d'occupation du canal
Les autres restent en silence pendant cette période

Scénarios

RTS/CTS est optionnel



NAV (Network Allocation Vector) : Virtual Carrier Sense
Dans RTS, on a la durée d'occupation du canal
On vérifie plus le canal pendant cette période

Deux types de Carrier Sense dans le WiFi :

- Physical Carrier Sense : la couche physique mesure l'énergie du canal
- Virtual Carrier Sense : la couche MAC lit l'en-tête des trames reçues (le champ **Duration**) et réserve virtuellement le canal pour une durée donnée (NAV)

$NAV > 0$, on ne peut pas transmettre

$NAV = 0$, mais canal occupé, on ne peut pas transmettre

$NAV = 0$ et canal libre, on peut essayer de transmettre

IEEE 802.11 : DCF

Message de diffusion (Broadcast)

- 1 émetteur, plusieurs récepteurs

Problème ?

Message de diffusion (Broadcast)

- 1 émetteur, plusieurs récepteurs
- Si tous les récepteurs ACK après SIFS -> collisions inévitables

Donc, les messages broadcast ne sont transmis qu'une seule fois, en utilisant la valeur minimale de la fenêtre de contention, et leur transmission n'est pas fiable.

Pourquoi observe-t-on toujours des collisions avec CSMA/CA ?

- Le mécanisme CA permet de réduire les collisions, mais ne peut pas les éliminer totalement
- La probabilité de collision dépend de deux facteurs principaux :
 - Le nombre de stations en compétition pour accéder au canal
 - La taille de la fenêtre de contention
- Une fenêtre de contention plus grande diminue la probabilité de collision, mais augmente le délai moyen (back-off)

IEEE 802.11 : DCF

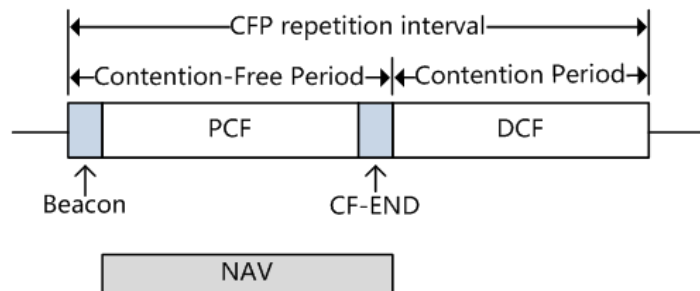
Conclusion :

- Un mécanisme d'accès au canal **décentralisé**
- **Peu performant** en situation de mobilité
- **Sature** dans les environnements denses

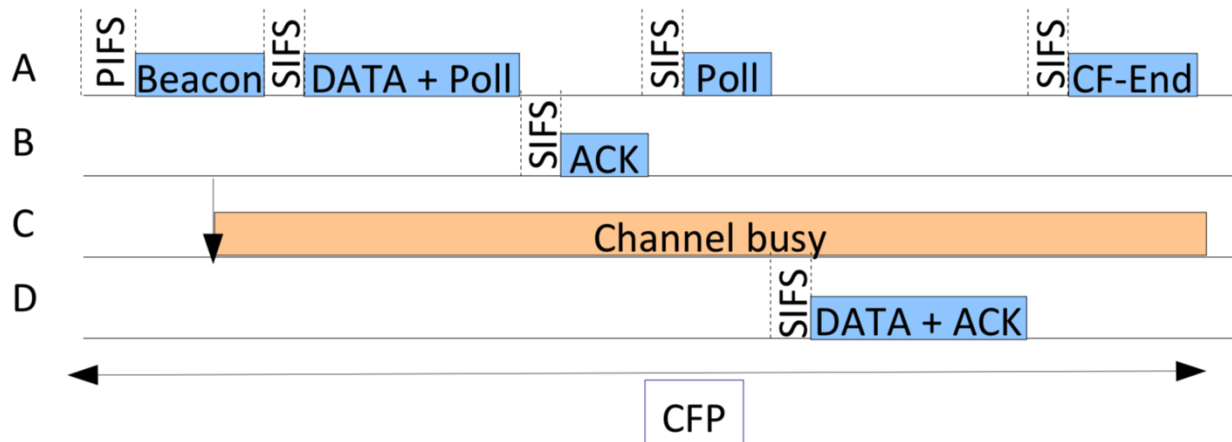
IEEE 802.11 : PCF

PCF (Point Coordination Function)

- Protocole de transfert de trames sans contention (Contention-Free)
- Basé sur un mécanisme de polling effectué par l'AP
- Coexiste avec le DCF

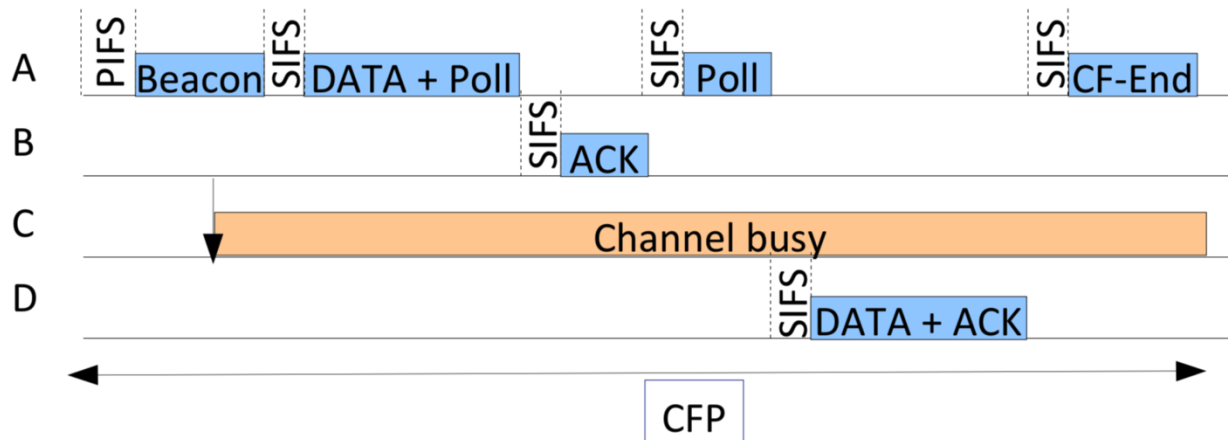


IEEE 802.11 : PCF



IEEE 802.11 : PCF

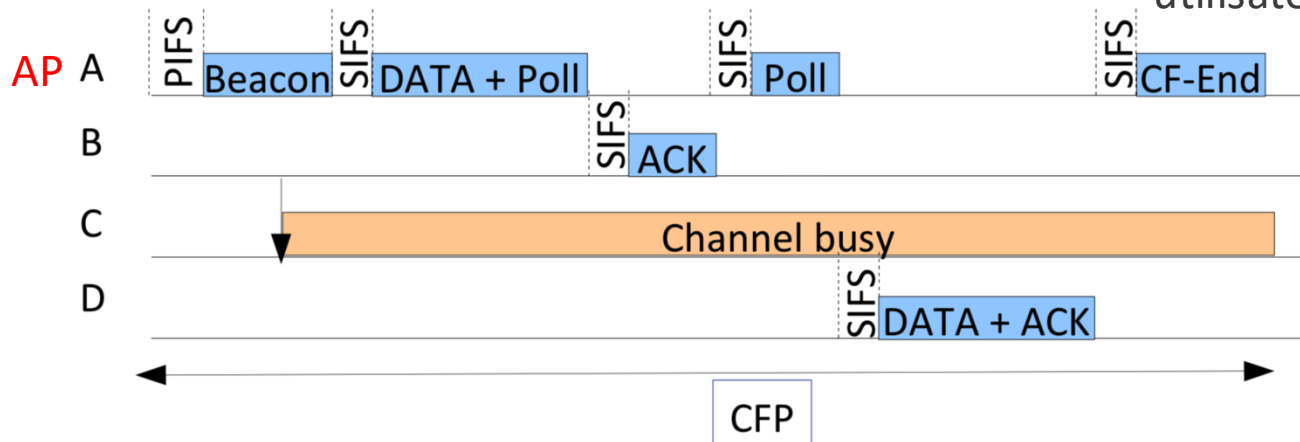
Qui est AP ?



IEEE 802.11 : PCF

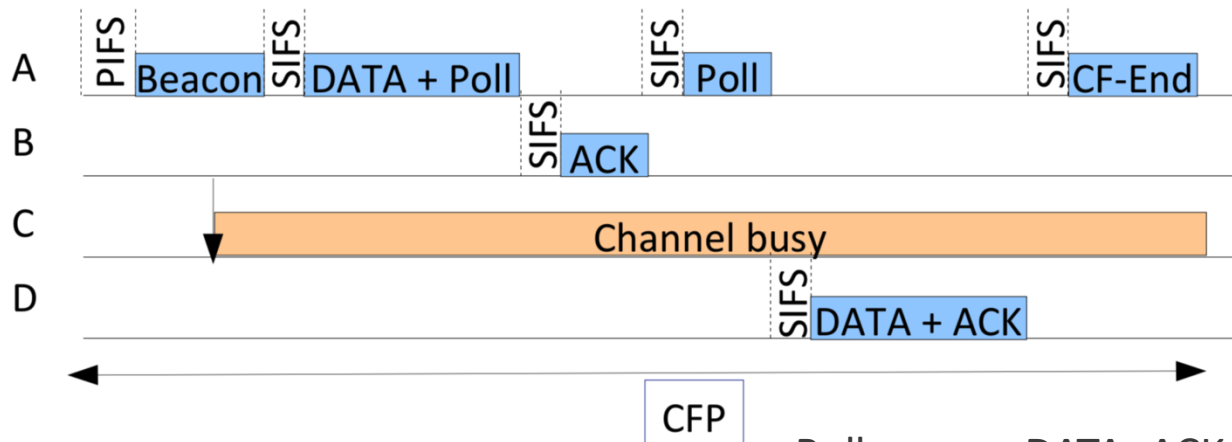
Beacon après un PIFS pour annoncer le début d'une CFP

Trames de Poll successives
Pas forcément tous les utilisateurs



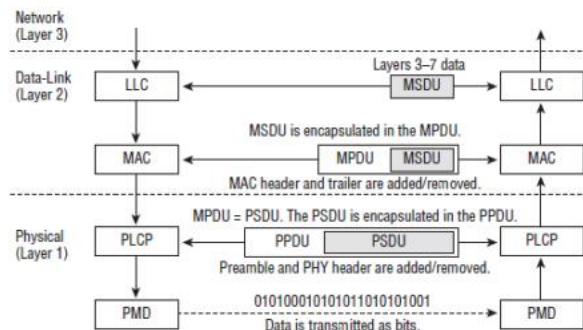
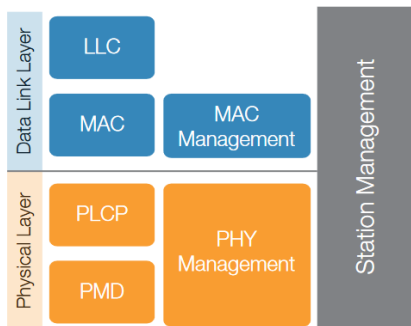
IEEE 802.11 : PCF

Poll reçu -> un ACK après un SIFS, si on n'a des données à envoyer



Poll reçu -> DATA+ACK après un SIFS,
Si on a des données à transmettre

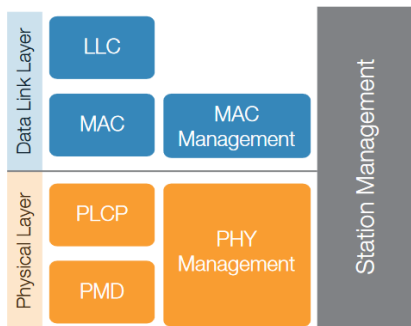
IEEE 802.11 : architecture protocolaire



La couche PHY est divisée en deux sous-couches : PLCP et PMD

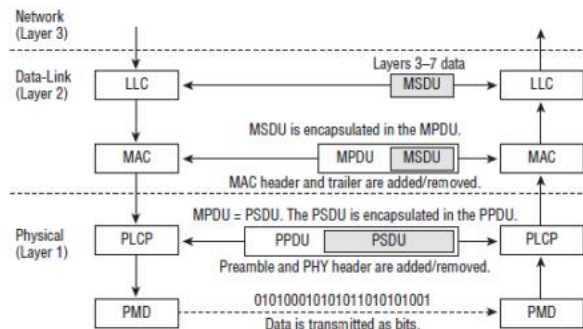
- PLCP (Physical Layer Convergence Procedure)
 - La trame MAC (**MPDU** : MAC Protocol Data Unit) est transmise au PLCP.
 - Dans le point de vue du PLCP, cette **MPDU** est appelée **PSDU** (PLCP Service Data Unit).
 - PLCP encapsule cette **PSDU** dans une trame physique (PPDU : Physical layer PDU), en ajoutant :
 - Un préambule pour la synchronisation
 - Un en-tête PLCP (PLCP Header) avec la longueur, le débit et d'autres paramètres (**MCS**)

IEEE 802.11 : architecture protocolaire



La couche PHY est divisée en deux sous-couches :
PLCP et PMD

- PMD (Physical Medium Dependent)
- Le PMD prend le **PPDU** créé par le PLCP, le **module** puis le **transmet sous forme de bits** sur l'interface radio

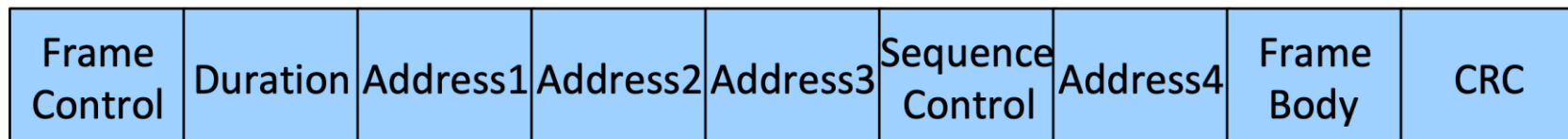


- Réalise la modulation
- Effectue le codage et décodage
- Convertit les bits - signaux électromagnétiques
- Gère les paramètres physiques (puissance, fréquence, bande passante, etc.)

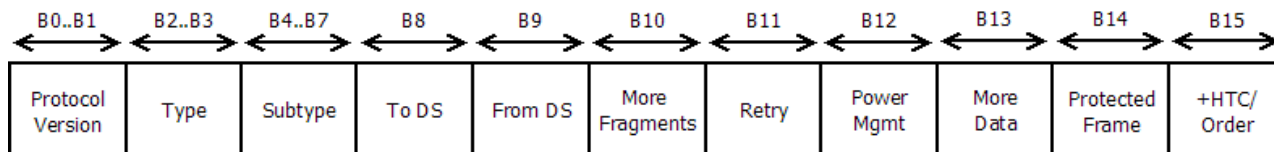
IEEE 802.11 : trame MAC

Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4	Frame Body	CRC
---------------	----------	----------	----------	----------	------------------	----------	------------	-----

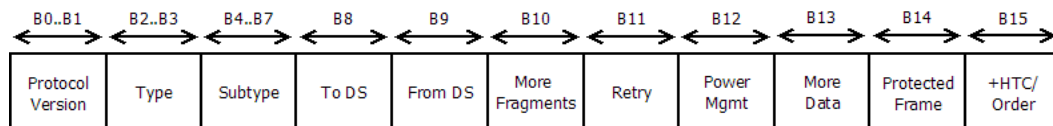
IEEE 802.11 : trame MAC



Frame Control (2 octets) : les informations sur le type, le rôle de la trame et des options de gestion du protocole



IEEE 802.11 : trame MAC



- Protocol Version : 0 – WLAN (a/b/g/n/ac/ax...), 1 – ah (Low Power, IoT)
- Type : 00 – Management, 01 – Control, 10 – Data, 11 – Extension
- Subtype : Préciser la fonction de la trame (Beacon, RTS/CTS, ACK, Data, Poll, ...)
- **To DS : Indiquer si la trame est destinée au DS (à travers un AP)**
- **From DS : Indiquer si la trame provient du DS**
- More Fragments : Indiquer s'il existe encore des fragments appartenant à la même trame
- Retry : Signaler que la trame est une retransmission d'une trame précédente
- Power Mgmt : Indiquer si la station entre en mode veille après cette trame
- More Data : Indiquer que l'émetteur a encore des trames à envoyer
- Protected Frame : Indiquer que la trame est chiffrée
- HTC/Order : Indiquer s'il existe le champ HTC (High Throughput Control)

IEEE 802.11 : trame MAC

Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4	Frame Body	CRC
---------------	----------	----------	----------	----------	------------------	----------	------------	-----

Duration (2 octets) : la durée pendant laquelle le canal sera utilisé pour la transmission en cours et les trames associées

Informers les autres stations du réseau qu'elles doivent attendre avant d'émettre, afin d'éviter les collisions.

-> Mettre à jour le compteur NAV

IEEE 802.11 : trame MAC

Frame Control	Duration	Address1	Address2	Address3	Sequence Control	Address4	Frame Body	CRC
---------------	----------	----------	----------	----------	------------------	----------	------------	-----

Address (6 octets) 1-4

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source

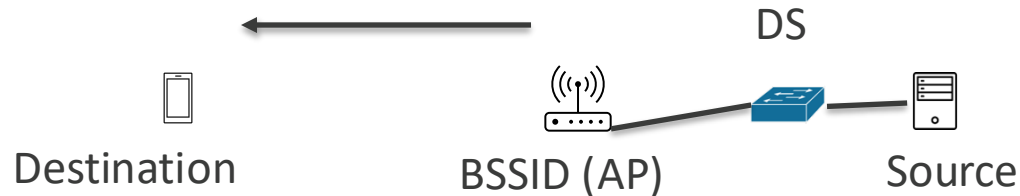
IEEE 802.11 : trame MAC

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source

Mode IBSS : pas de AP, le BSSID est généré aléatoirement

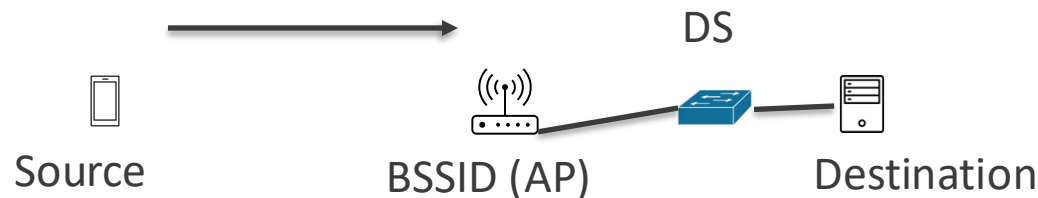
IEEE 802.11 : trame MAC

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source



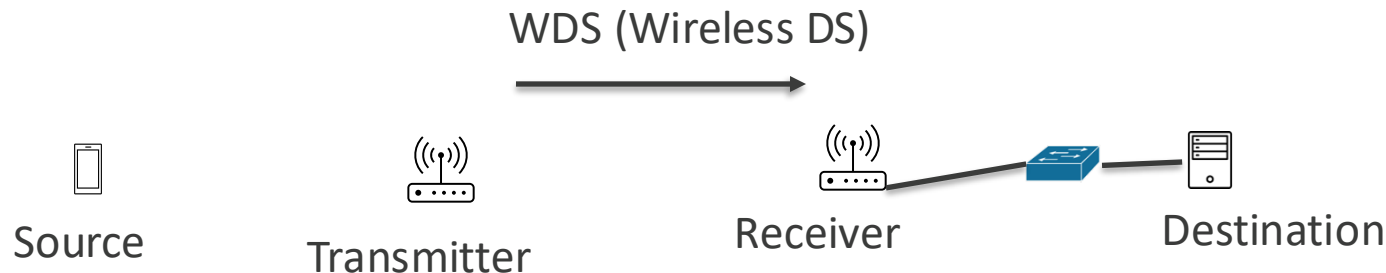
IEEE 802.11 : trame MAC

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source



IEEE 802.11 : trame MAC

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source



IEEE 802.11 : trame MAC

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Receiver	Transmitter	Destination	Source

Si Address 4 est N/A, ce champ n'est pas présent dans l'en-tête

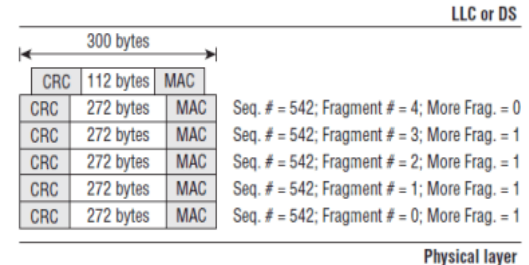
IEEE 802.11 : trame MAC



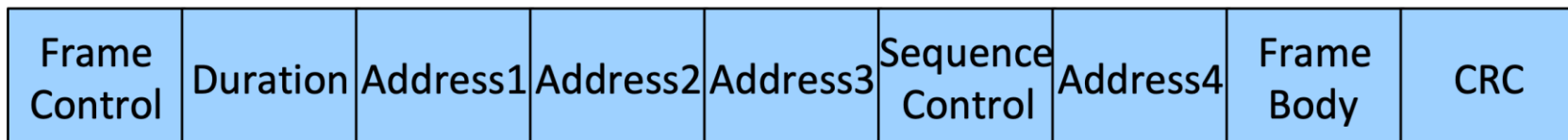
Sequence Control (2 octets) : Fragment Number (4 bits), Sequence Number (12 bits)

- Fragment Number : Numéro de fragment, identifie la partie d'une trame fragmentée
- Sequence Number : Numéro de séquence de la trame, identifie l'ordre de l'envoi

FIGURE 3.32 MSDU fragmentation



IEEE 802.11 : trame MAC



Frame Body : Données utiles, MSDU, 0 – 2312 octets (selon le type de trame)

CRC (4 octets) : contrôler l'intégrité de la trame

Résumé (Cours 4)

- Ondes électromagnétiques & propagation
- CSMA/CA
- RTS/CTS
- IEEE 802.11
- DCF/PCF