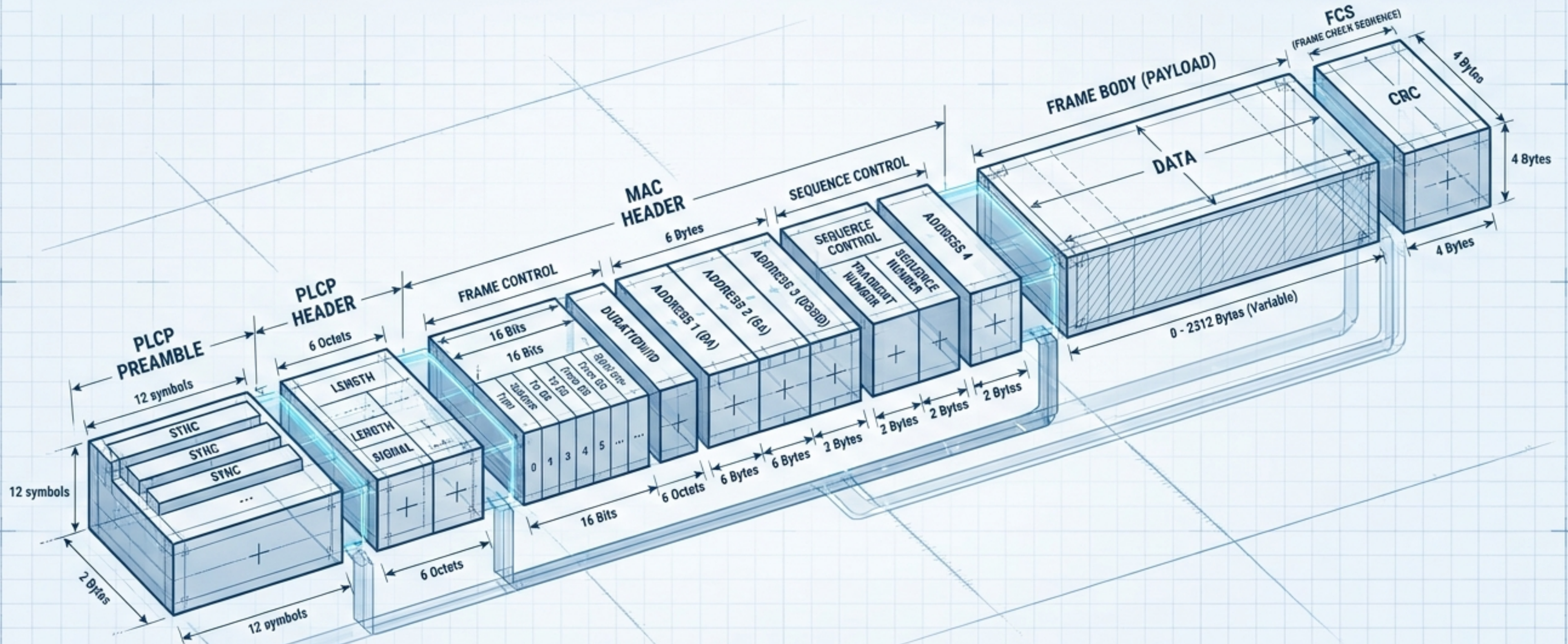
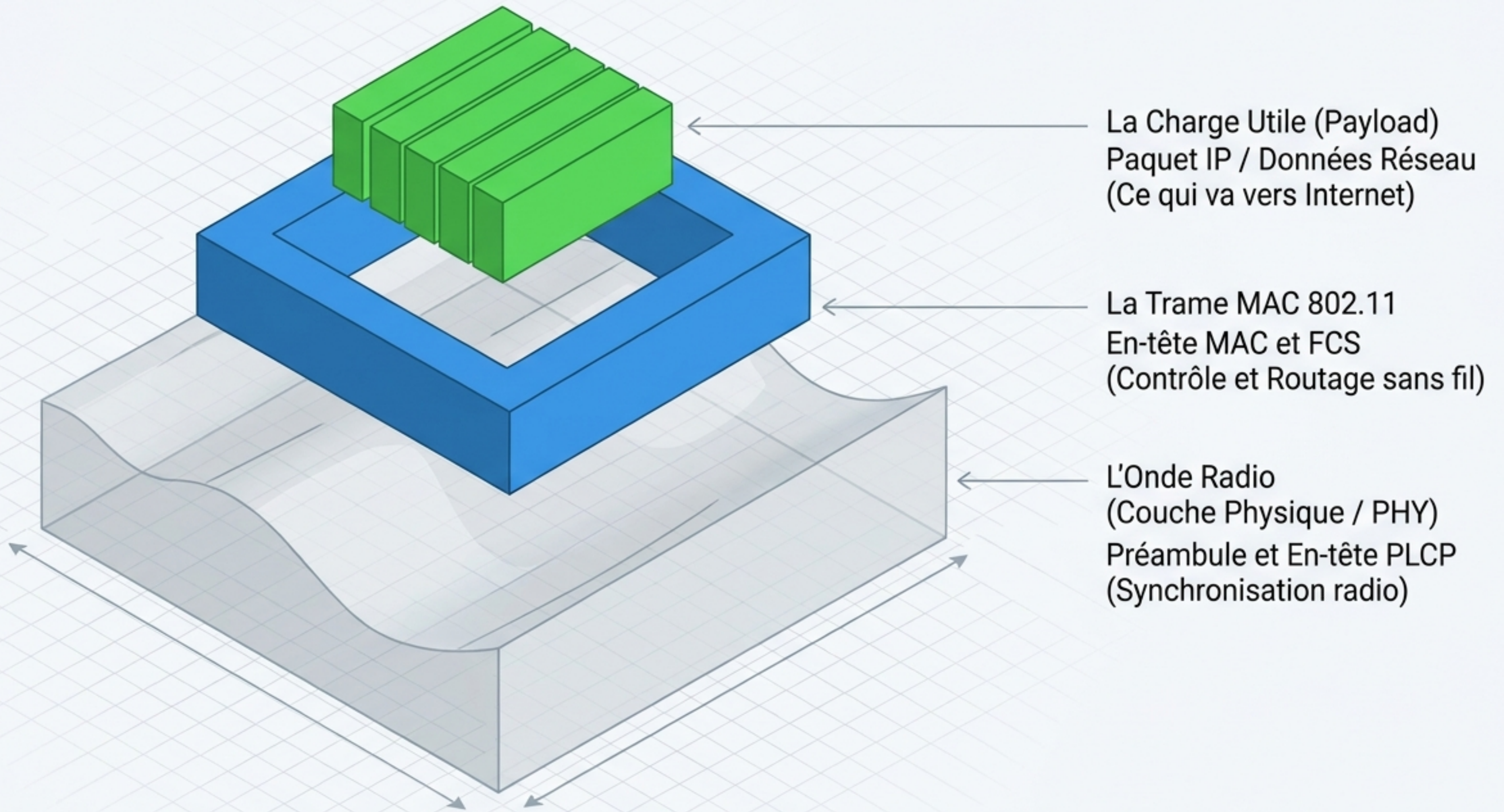


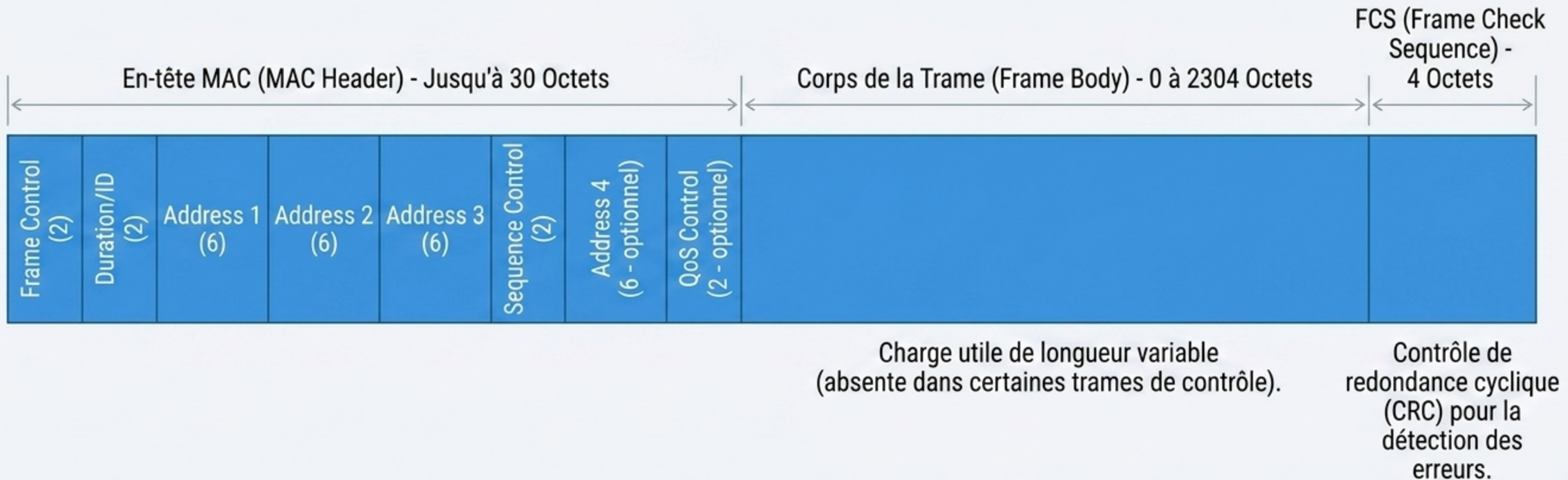
Radiographie du Wi-Fi : L'Anatomie des Trames 802.11

Un guide visuel de l'architecture, de la taxonomie et du contenu des trames sans fil.





Contrairement à l'Ethernet, le sans-fil nécessite une infrastructure complexe de contrôle intégrée directement dans la trame MAC pour survivre dans l'air.



Chaque trame 802.11, qu'elle transporte une vidéo HD ou un simple accusé de réception, partage ce squelette fondamental.

Bits 0-1 : Protocol Version
(Toujours 00 pour le WLAN standard)

Bits 2-3 : Type
(Détermine la catégorie :
00=Gestion, 01=Contrôle,
01=Contrôle, 10=Données)

Bits 8-9 : To DS / From DS
(Indicateurs de direction)

Bits 10-15 : Drapeaux d'état
(More Fragments, Retry, Power Management,
More Data, Protected Frame, Order)

Core Focus

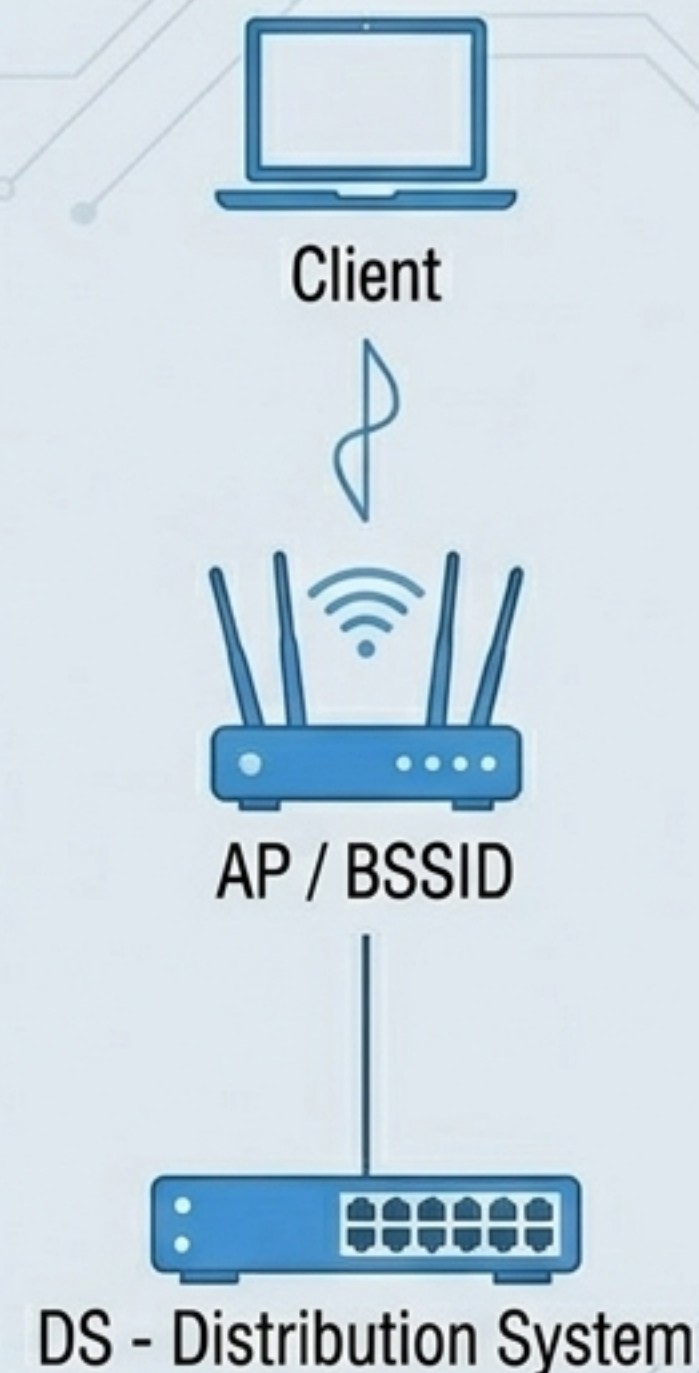


Bits 2-3 : Type
(Détermine la catégorie :
00=Gestion,
01=Contrôle,
10=Données)

Bits 4-7 : Subtype
(Définit la fonction exacte,
ex: Beacon, ACK)

Bits 10-15 : Drapeaux d'état
(More Fragments, Retry, Power
Fragmenets, Retry, Power Management,
More Data, Protected Frame, Order)

	From DS (0)	From DS (1)
To DS (0)	<p>Ad-Hoc / BSS Interne</p> <p>Adr 1 = Destination (DA)</p> <p>Adr 2 = Source (SA)</p> <p>Adr 3 = BSSID</p> <p>Pas de passage par le réseau filaire.</p>	<p>Depuis le DS vers le Client</p> <p>Adr 1 = Destination (DA)</p> <p>Adr 2 = BSSID (Transmetteur)</p> <p>Adr 3 = Source (SA)</p> <p>Téléchargement depuis Internet.</p>
To DS (1)	<p>Du Client vers le DS</p> <p>Adr 1 = BSSID (Récepteur)</p> <p>Adr 2 = Source (SA)</p> <p>Adr 3 = Destination (DA)</p> <p>Envoi vers Internet.</p>	<p>Pont Sans Fil / Mesh</p> <p>Utilise les 4 adresses (Récepteur, Transmetteur, Destination, Source).</p> <p>Communication entre Points d'Accès.</p>



Trames de Gestion (Management)

Bits Type : 00

- Rôle : Établir et maintenir les connexions. Les règles du réseau.
- Charge utile : Informations réseau (SSID, capacités), pas de données utilisateur.

Trames de Contrôle (Control)

Bits Type : 01

- Rôle : Gérer l'accès au support physique et éviter les collisions. Les agents de circulation.
- Charge utile : Aucune. Juste des en-têtes MAC rapides.

Trames de Données (Data)

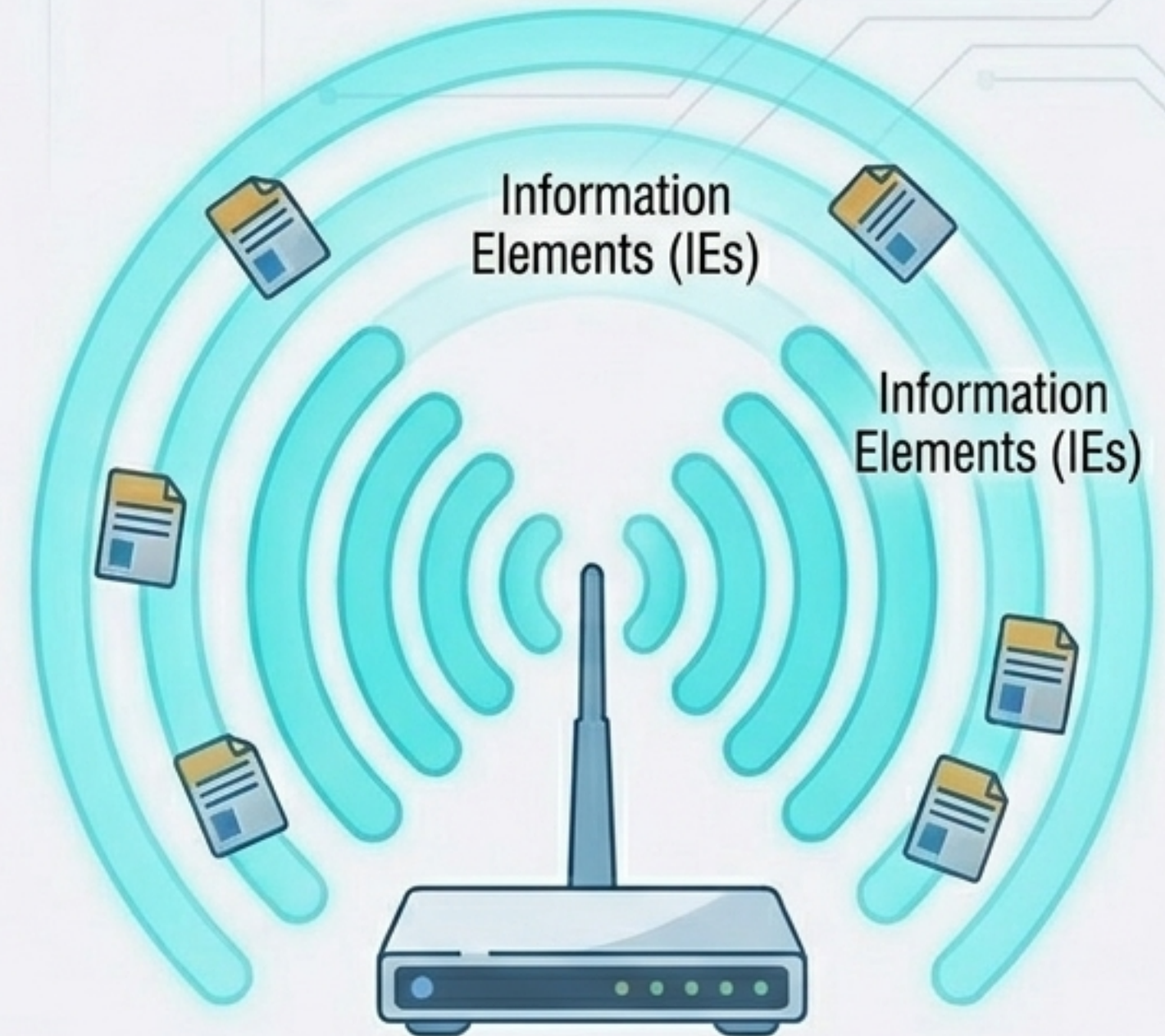
Bits Type : 10

- Rôle : Transporter la charge utile. Les camions de livraison.
- Charge utile : Paquets réseau (IP, TCP, vidéo, web).

Les deux bits du champ 'Type' dictent le comportement absolu de la trame.

Les Sous-types Fréquents (Type 00)

1000	: Beacon (Balise)
0100 / 0101	: Probe Req/Resp (Sondage)
1011	: Authentication (Authentification)
0000 / 0001	: Association Req/Resp
1100	: Deauthentication (Déconnexion)



Les trames de gestion ne sont pas chiffrées par défaut (sauf 802.11w). Elles diffusent l'identité du réseau (SSID), les vitesses supportées et gèrent le cycle de vie de la connexion.

Découverte Passive - Le Phare



- Trame : Beacon (Sous-type 1000)
- Fréquence : Diffusé typiquement toutes les 102.4 ms (10 fois par seconde).
- Contenu : SSID, Horodatage, BSSID.

Découverte Active - Le Sonar



- Trames : Probe Request (0100) / Probe Response (0101)
- Mécanisme : Le client cherche activement des réseaux connus ou diffuse une requête générique pour cartographier la zone.



Client



AP

Étape 1 : Authentification Ouverte

Auth Request (Sous-type 1011) : Puis-je parler avec vous ?

Auth Response : Oui, votre identité MAC est acceptée.

Étape 2 : Association

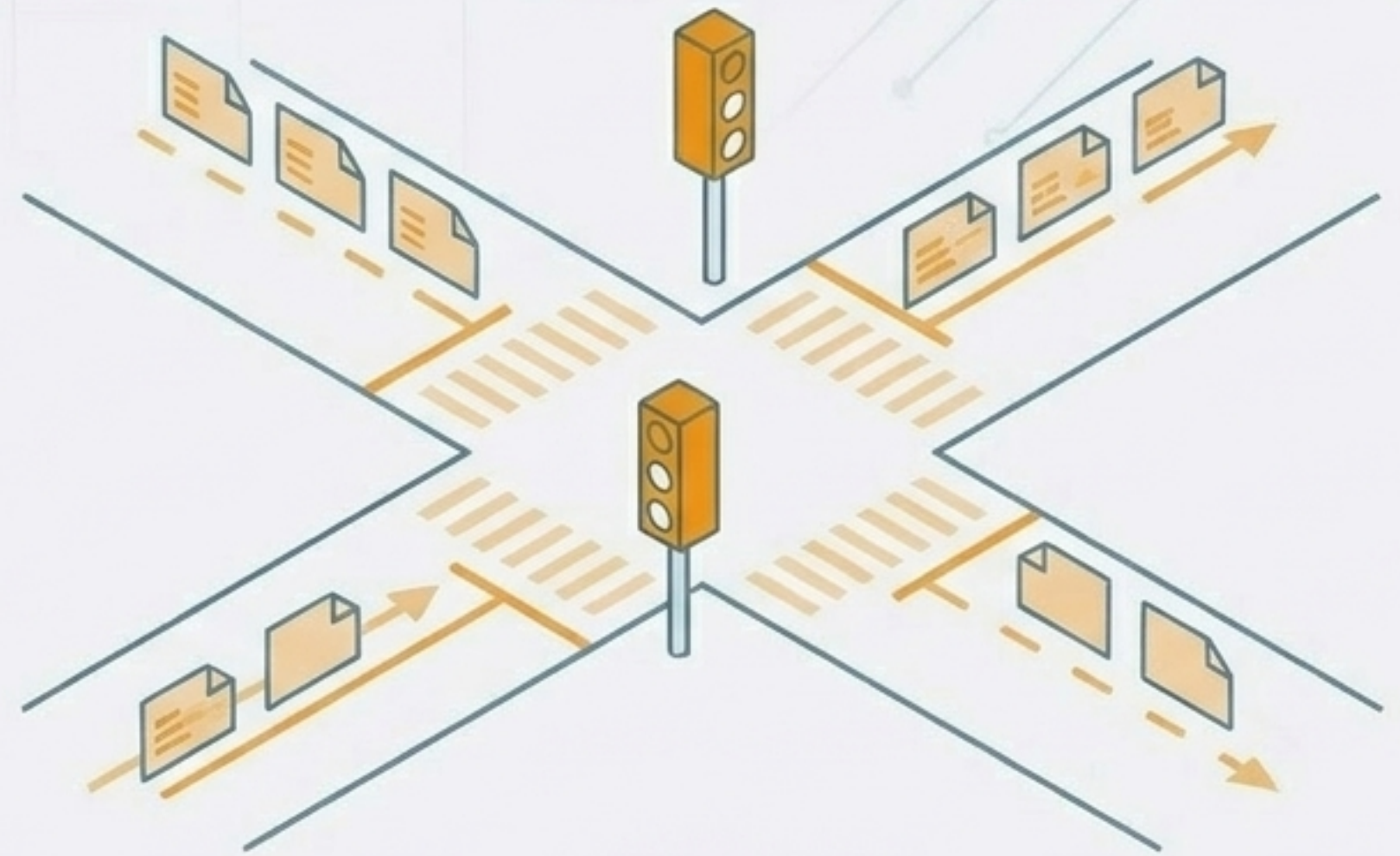
Assoc Request (Sous-type 0000) : Je veux rejoindre ce BSSID avec ces capacités réseau.

Assoc Response (Sous-type 0001) : Bienvenue. Voici votre AID (Association ID).

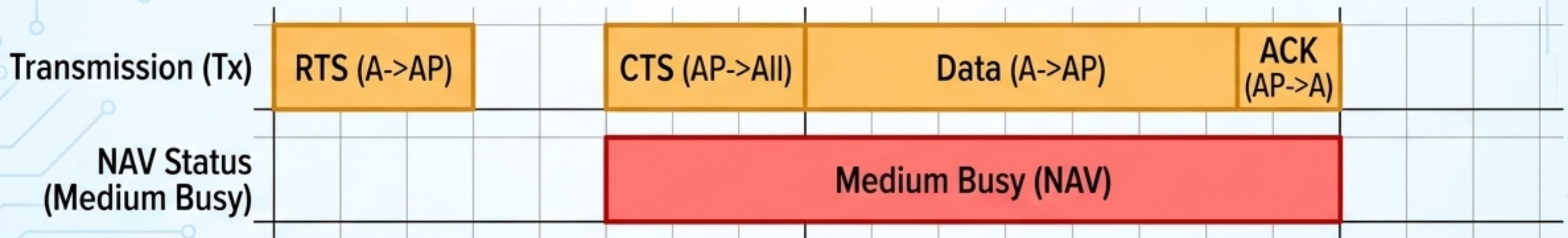
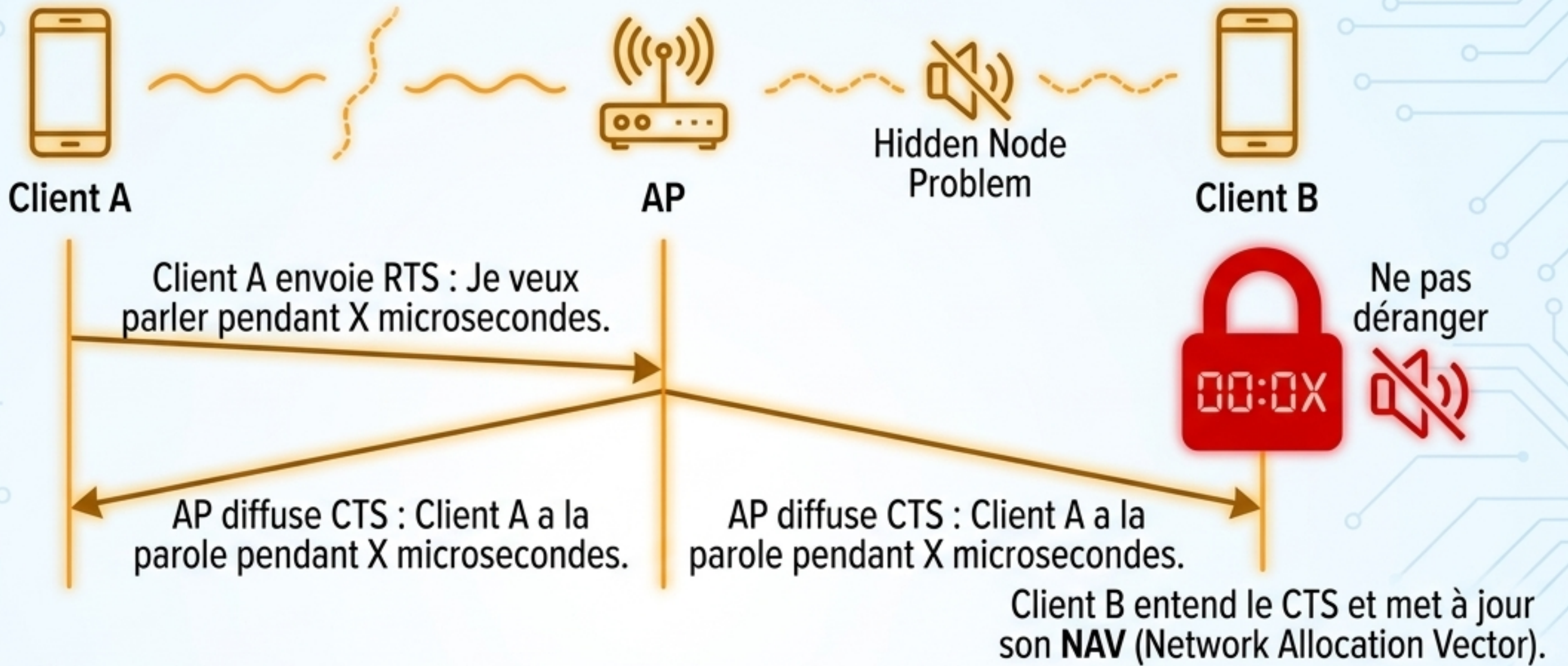
Dans le Wi-Fi 802.11, l'authentification précède toujours l'association.
Une station doit être authentifiée avant de pouvoir s'associer.

Les Sous-types Fréquents (Type 01)

- **1011** : RTS (Request to Send)
- **1100** : CTS (Clear to Send)
- **1101** : ACK (Acknowledgment)
- **1001** : Block ACK
- **1010** : PS-Poll (Power Save Poll)



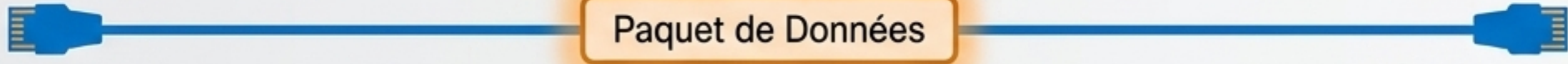
Ces trames sont minuscules, sans charge utile, et utilisent des espaces inter-trames très courts (SIFS) pour obtenir un accès prioritaire et exclusif au support.



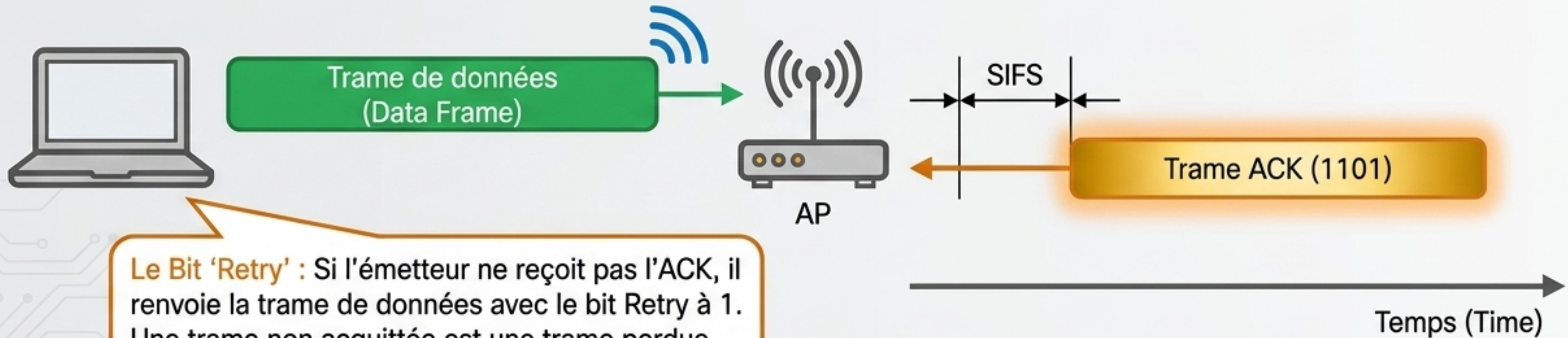
Le NAV agit comme un verrouillage matériel temporaire explicitement lié au champ Duration de l'en-tête MAC.

Ethernet : Envoyer et oublier

Pas d'accusé de réception (ACK) requis au niveau de la couche liaison de données.



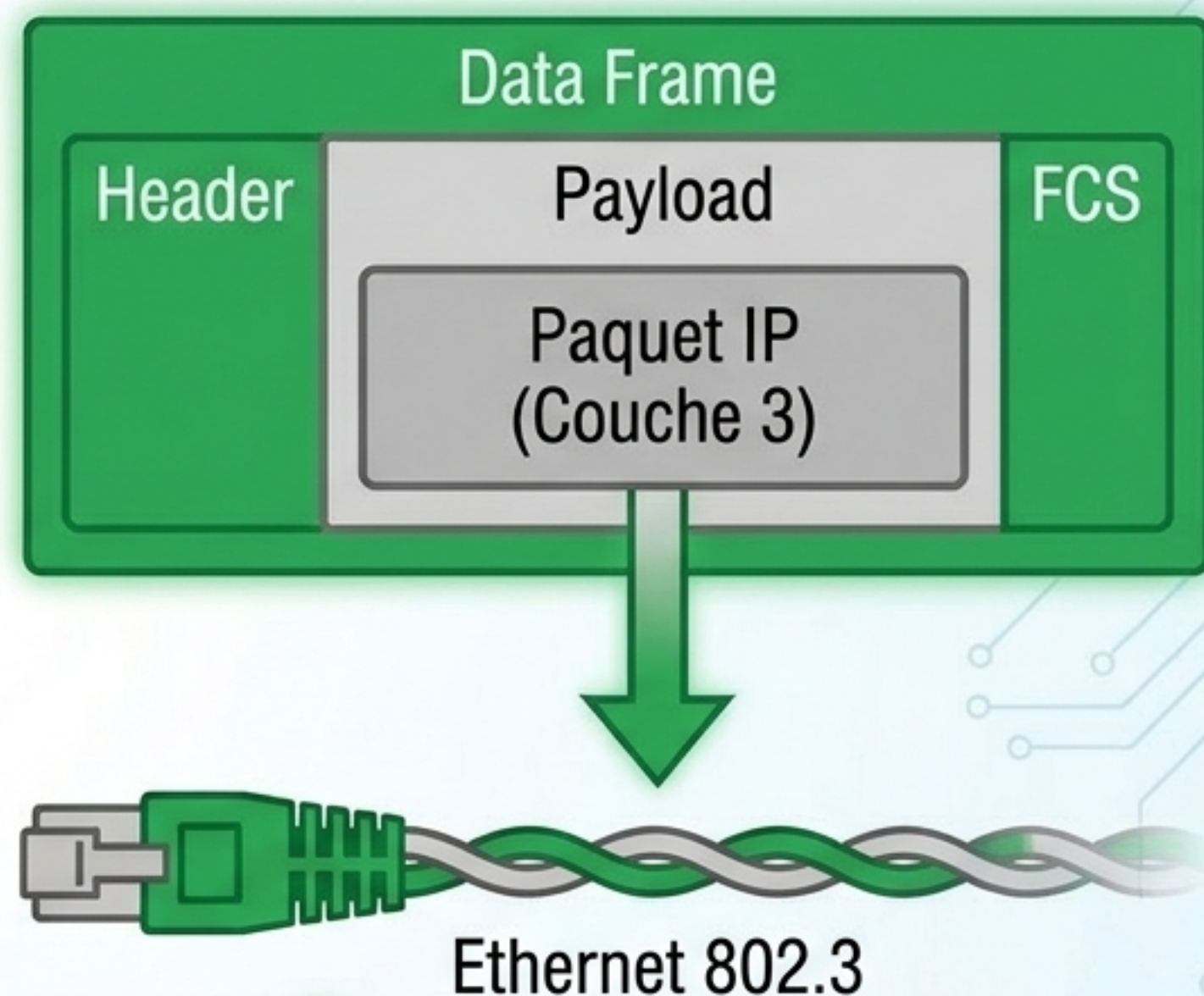
Wi-Fi : Faire confiance mais vérifier



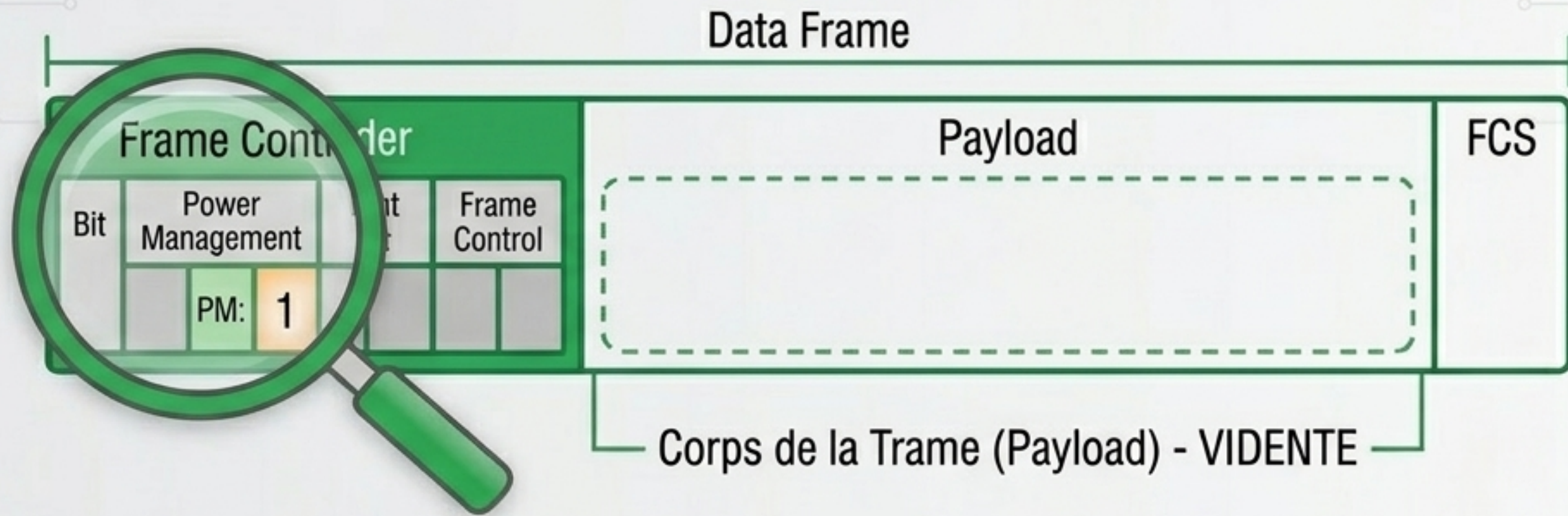
Le Bit 'Retry' : Si l'émetteur ne reçoit pas l'ACK, il renvoie la trame de données avec le bit Retry à 1. Une trame non acquittée est une trame perdue.

Les Sous-types Fréquents (Type 10)

- 0000 : Data (Données standard)
- 1000 : QoS Data (Données avec priorité)
- 0100 : Null (Pas de données)
- 1100 : QoS Null



C'est la seule catégorie de trame qui franchit la frontière entre le monde sans fil (802.11) et le réseau filaire (Ethernet 802.3). Tout le reste reste dans l'air.

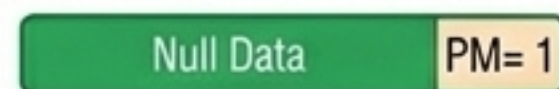


Le Paradoxe : Pourquoi envoyer une trame de données sans données ?

1.

Le client veut s'endormir pour économiser sa batterie.

2.



Il envoie une trame Null Data (0100) avec le bit Power Management défini sur 1.

3.



L'AP accuse réception et commence à mettre en mémoire tampon les données destinées au client endormi.

4.

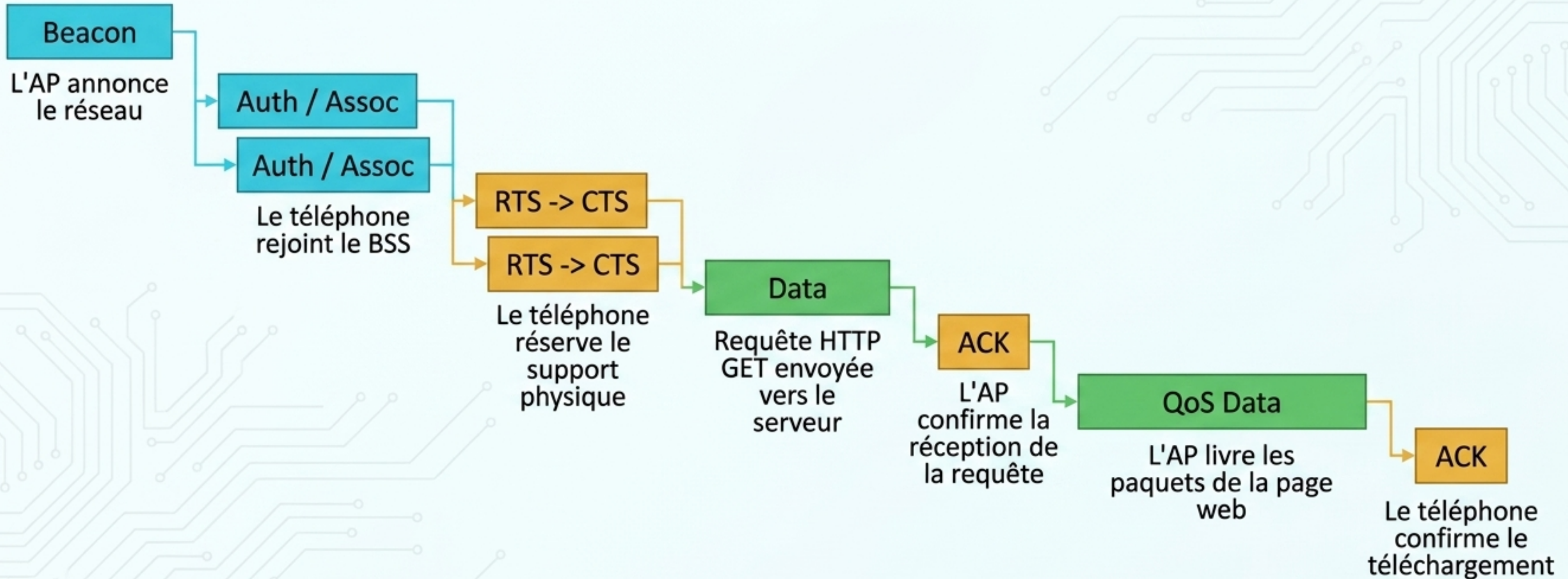


Le client se réveille plus tard avec une trame PS-Poll pour récupérer ses paquets en attente.

Aucune charge utile n'est gaspillée, la bande passante est préservée, la batterie est sauvée.

Synthesis

La Symphonie des Trames : Chargement d'une Page Web



Une simple requête web nécessite une cascade parfaitement chorégraphiée de trames de gestion, de contrôle et de données. C'est l'architecture invisible du Wi-Fi.